

Privacy Policy

Last updated: 29 April 2026

Operator: ADHD Entrepreneur Ventures LLC, a Wyoming limited liability company (mailing address in Texas) ("Company", "TAE", "we", "us", "our").

Address: 701 Tillery Street Unit 12 Suite 3474, Austin, TX 78702, United States of America.

Contact for privacy matters: contact@adhdinbiz.com

Website: <https://adhdinbiz.com> or <http://adhdentrepreneur.io>

1. SCOPE AND APPLICATION

This Privacy Policy describes how Company collects, uses, discloses, retains, and protects personal information (referred to in some jurisdictions as "personal data") in connection with:

- (a) Company's website at <https://adhdinbiz.com>, <http://adhdentrepreneur.io> and any successor or affiliated domain ("Website");
- (b) Company's programs, memberships, coaching engagements, and digital products ("Services");
- (c) Communications between Company and prospective, current, or former clients, applicants, contractors, and other counterparties.

This Policy applies to information about (i) individual visitors to the Website; (ii) authorised representatives of business clients (Company's clients are businesses, not consumers — see Section 2.4 below); (iii) prospective clients who interact with Company's marketing or sales channels; and (iv) other identifiable individuals whose data Company processes.

This Policy does not apply to third-party websites, services, or applications linked from the Website. Company is not responsible for the privacy practices of those third parties.

2. ROLES AND LEGAL FRAMEWORK

2.1 Controller

For the purposes of the EU General Data Protection Regulation ("GDPR"), the United Kingdom GDPR ("UK GDPR"), and equivalent data protection laws, ADHD Entrepreneur Ventures LLC is the **controller** of personal data processed under this Policy.

2.2 Applicable laws

Company processes personal data in accordance with the following laws to the extent each applies based on the data subject's location and the nature of processing:

- (a) The EU GDPR (Regulation (EU) 2016/679) and applicable Member State implementing laws;
- (b) The UK GDPR and the Data Protection Act 2018;
- (c) The California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA/CPRA");
- (d) Other applicable U.S. state privacy laws (including without limitation the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Texas Data Privacy and Security Act);
- (e) The Australian Privacy Act 1988 and the Australian Privacy Principles ("APPs") set out in Schedule 1 of that Act;
- (f) Other applicable data protection or privacy laws in jurisdictions where Company processes personal data.

2.3 EU/UK representative

Company does not currently maintain a dedicated EU/UK Article 27 representative. Where the limited derogation in Article 27(2) of the EU/UK GDPR applies (occasional processing, no large-scale processing of special categories, low risk to data subjects' rights), no representative is required. Inquiries from EU/UK data subjects should be directed to contact@adhdinbiz.com.

2.4 B2B context

Company contracts with businesses, sole traders, and partnerships in the course of their trade or profession — not with consumers. Where this Policy refers to "Clients," the term means the business entity or sole trader. Personal data of authorised representatives of those businesses is processed under this Policy in the business-to-business (B2B) context. Nothing in this Policy is intended to imply or create consumer-protection obligations beyond those non-waivable under applicable law.

3. CATEGORIES OF PERSONAL INFORMATION COLLECTED

Company collects the following categories of personal information:

3.1 Identifiers and contact information

Full name; business name; business address; email address; phone number; country of business; time zone; signatory name and title; payment-method billing address.

3.2 Account and program participation data

Program or membership enrolment status; payment plan; participation history; attendance records; course/module progress; community-platform username and avatar; submitted forms (intake forms, application forms, feedback forms).

3.3 Commercial information

Products and services purchased; transaction history; payment dates and amounts; refund requests; chargebacks; payment-plan status.

3.4 Payment and billing data

Payment-method type (the last four digits of payment card may be stored; full card numbers are not stored by Company — they are processed by our payment processors); billing currency; transaction identifiers issued by payment processors; reserve amounts (where applicable, e.g., Splitit).

3.5 Communications data

Emails to/from Company; chat messages in Company-administered community platforms; voice and video recordings of group calls, workshops, and live events

(with notice and consent per the applicable Master Services Agreement); meeting notes; AI-generated meeting transcripts and summaries.

3.6 Sensitive or special-category data

Client may voluntarily disclose information about their ADHD diagnosis, neurodivergence, mental-health status, family circumstances, or business challenges in the course of participating in coaching, group calls, or community discussions. Company does not require disclosure of such information and treats any disclosed sensitive information with elevated care, processing it only as necessary to deliver the Services or with explicit consent.

Under the EU/UK GDPR, ADHD-related health information may constitute a "special category" of personal data under Article 9. Company relies on explicit consent (Article 9(2)(a)) and, where applicable, the data subject's manifestly making such information public (Article 9(2)(e)) as the lawful basis for processing.

Under the Australian Privacy Act, such information may be "sensitive information" within the meaning of section 6, and Company processes it only with consent (APP 3.3).

3.7 Technical and Website data

IP address; device type; browser type and version; operating system; pages visited; referral URL; date and time of access; approximate geographic location derived from IP; cookie identifiers; analytics identifiers; session-replay data (if used).

3.8 Marketing data

Responses to marketing emails, advertisements, and surveys; engagement metadata (open, click, conversion events); ad-platform identifiers (if interest-based advertising is used).

3.9 Inferences

Company may derive inferences from the above categories about a data subject's preferences, engagement level, and likely interest in additional Company offerings, for the purposes of marketing and program-improvement.

Company does not engage in solely automated decision-making that produces legal or similarly significant effects on data subjects within the meaning of Article 22 of the EU/UK GDPR.

4. SOURCES OF PERSONAL INFORMATION

Company collects personal information from the following sources:

- (a) Directly from the data subject (e.g., when completing a Website form, signing up for a program, attending a coaching call, or sending an email);
- (b) From the Client business that the data subject represents;
- (c) From service providers (described in Section 6) that process data on Company's behalf;
- (d) From advertising partners and analytics providers, where data subjects have interacted with Company-related advertising;
- (e) From publicly available sources (e.g., LinkedIn business profiles), where Company researches prospective clients;
- (f) From referrals, where an existing Client refers a prospective Client.

5. PURPOSES OF PROCESSING AND LAWFUL BASES

Company processes personal information for the following purposes. For each purpose, the EU/UK GDPR lawful basis is identified.

#	Purpose	Lawful basis (EU/UK GDPR)
5.1	To enrol Clients in programs and memberships, and to deliver the Services contracted for	Article 6(1)(b) — performance of a contract
5.2	To process payments, manage payment plans, issue refunds, and recover overdue amounts	Article 6(1)(b) — contract; Article 6(1)(c) — legal obligation (tax / accounting)
5.3	To communicate with Clients about their account, schedule changes, billing, support, and program updates	Article 6(1)(b) — contract
5.4	To provide community-platform access and moderate community conduct	Article 6(1)(b) — contract; Article 6(1)(f) — legitimate interest in safe community
5.5	To record and distribute group calls and workshops to participants	Article 6(1)(b) — contract; Article 6(1)(a) — consent (where required)
5.6	To use Client testimonials in marketing	

		Article 6(1)(a) — consent; Article 6(1)(f) — legitimate interest in promoting the Services
5.7	To send marketing communications about TAE programs and memberships to existing Clients and (where permitted) prospects	Article 6(1)(f) — legitimate interest; Article 6(1)(a) — consent (where required by ePrivacy or local law)
5.8	To analyse Website usage and improve the Website and Services	Article 6(1)(f) — legitimate interest; Article 6(1)(a) — consent (for non-essential cookies)
5.9	To detect and prevent fraud, chargeback abuse, and unauthorised use of intellectual property	Article 6(1)(f) — legitimate interest
5.10	To comply with applicable law, respond to legal process, and enforce contracts	Article 6(1)(c) — legal obligation; Article 6(1)(f) — legitimate interest
5.11	To process sensitive information voluntarily shared during coaching	Article 6(1)(b) + Article 9(2)(a) — contract + explicit consent

For data subjects in the United States, equivalent purposes apply under CCPA/CPRA and other state privacy laws. For Australian data subjects, equivalent purposes apply under APP 3 and APP 6.

6. SHARING AND DISCLOSURE

Company discloses personal information only as follows:

6.1 Service providers (data processors)

Company engages third-party service providers to process personal data on Company's behalf. These service providers are bound by contract to use personal data only for the purposes Company specifies and to implement appropriate security measures. Categories include:

- **Payment processing and billing:** Whop, Splitit (for instalment-based payments), and any subsequent payment processor Company engages.
- **Customer relationship management and contract execution:** Go High Level ("GHL").
- **Community platform and program delivery:** Circle.so, Notion.

- **Email and calendaring:** Google Workspace (Gmail, Google Calendar, Google Drive).
- **Internal operations and project management:** Notion, Slack.
- **Workflow automation:** Make.com.
- **Spreadsheets and reporting:** Google Sheets.
- **Website hosting:** Wix (primary websites at adhdinbiz.com and adhdentrepreneur.io) and Go High Level ("GHL") (funnel pages, landing pages, and ancillary marketing pages).
- **Website analytics:** Google Analytics.
- **Advertising platform pixels and conversion tracking:** Meta (Facebook / Instagram) Pixel; Google Ads; TikTok Pixel.
- **AI transcription and call recordings:** Fathom (post-call transcription and summarisation); Zoom (live session hosting and recording, with native transcription where enabled).
- **Email marketing and broadcast communications:** Go High Level and Flodesk.
- Professional advisers (e.g., legal, accounting, tax, audit) under duties of confidentiality.

6.2 Legal disclosures

Company may disclose personal data where required by law, in response to a valid subpoena, court order, or other legal process, or to: (a) comply with a legal obligation; (b) protect Company's rights, property, or safety, or those of Clients or third parties; (c) detect, prevent, or address fraud, security, or technical issues; or (d) enforce Company's contracts, including this Policy and the Master Services Agreement.

6.3 Business transfers

If Company is involved in a merger, acquisition, financing, asset sale, or other business transaction, personal data may be transferred to a successor or acquirer, subject to appropriate confidentiality and continued application of this Policy (or a successor policy on no less protective terms).

6.4 With consent

Company may share personal data with other parties (e.g., featured guest experts, joint-venture partners) where the data subject has given specific consent.

6.5 No sale of personal information

Company does not "sell" personal information for monetary consideration within the meaning of CCPA/CPRA. Where Company shares personal data with advertising partners for cross-context behavioural advertising (which may constitute "sharing" under CCPA/CPRA), Company will provide and honour an opt-out mechanism in accordance with Section 9.4.

7. INTERNATIONAL DATA TRANSFERS

Company is established in the United States. Personal data of data subjects located outside the United States is transferred to and processed in the United States and other jurisdictions where Company's service providers operate.

7.1 Transfers from the EU/EEA and UK

For transfers of personal data from the European Economic Area or the United Kingdom to the United States, Company relies on:

- (a) The European Commission's Standard Contractual Clauses (Module 1 controller-to-controller; Module 2 controller-to-processor) and the UK International Data Transfer Addendum, where applicable, with each service provider; and/or
- (b) The EU–US Data Privacy Framework ("DPF") and the UK Extension to the DPF, where the recipient is DPF-certified.

A copy of the SCCs and any supplementary measures applicable to a specific transfer is available on request to contact@adhdinbiz.com.

7.2 Transfers from Australia

For transfers of personal data of Australian data subjects, Company complies with APP 8 by ensuring that overseas recipients are subject to a law or binding scheme substantially similar to the APPs, or by obtaining the data subject's consent after notifying them of the consequences of consent.

7.3 Transfers from other jurisdictions

Where personal data is transferred from any other jurisdiction with cross-border transfer restrictions, Company implements transfer mechanisms required by that jurisdiction's law.

8. RETENTION

Company retains personal data only for as long as reasonably necessary for the purposes set out in Section 5, after which it will be deleted, anonymised, or aggregated. Specific retention periods include:

- **Active client records:** For the duration of the program or membership, plus seven (7) years following termination, to satisfy Wyoming and U.S. federal record-keeping, audit, and limitation-period requirements.
- **Financial and tax records:** Seven (7) years from creation, in accordance with U.S. and applicable foreign tax-record retention requirements.
- **Marketing data for unsubscribed contacts:** Suppression-list data is retained indefinitely to honour opt-out preferences.
- **Marketing data for engaged prospects:** Up to thirty-six (36) months following last engagement, after which the record is deleted or anonymised.
- **Recordings of group calls:** Up to thirty-six (36) months from the date of recording, unless deleted earlier on request or extended for archival/training purposes.
- **Website analytics:** Per the retention configured with the analytics provider — typically not more than twenty-six (26) months for granular event data.
- **Legal-claim related data:** Until the resolution of the relevant claim and the expiry of any applicable limitation period.

Longer retention applies where required by applicable law, court order, or to support a pending or anticipated legal claim.

9. RIGHTS OF DATA SUBJECTS

Depending on the jurisdiction in which a data subject is located, the following rights may apply:

9.1 EU / UK GDPR rights

Data subjects in the EU/EEA or UK have the right to: (a) access personal data Company processes about them (Article 15); (b) rectify inaccurate personal data (Article 16); (c) erasure (the "right to be forgotten") subject to applicable conditions (Article 17); (d) restrict processing (Article 18); (e) data portability for data processed by automated means under contract or consent (Article 20); (f) object to processing based on legitimate interests, including direct marketing (Article 21); (g) withdraw consent at any time, without affecting the lawfulness of pre-withdrawal processing (Article 7(3)); and (h) lodge a complaint with the supervisory authority in their EU Member State of habitual residence, place of work, or place of the alleged infringement (or with the UK Information Commissioner's Office for UK data subjects).

9.2 California (CCPA/CPRA) rights

California residents have the right to: (a) know the categories of personal information collected, the sources, the purposes, and the categories of third parties with whom it is shared; (b) access the specific pieces of personal information collected; (c) deletion, subject to applicable exceptions; (d) correction of inaccurate personal information; (e) opt-out of "sale" or "sharing" of personal information; (f) limit use and disclosure of sensitive personal information to that necessary to provide the requested service; and (g) non-discrimination for exercising any of these rights.

9.3 Other U.S. state rights

Residents of Virginia, Colorado, Connecticut, Utah, Texas, and other states with comprehensive privacy laws have rights substantially similar to those in Section 9.2, subject to each state's specific provisions and thresholds.

9.4 Australian rights

Australian data subjects have the right to: (a) request access to personal information Company holds about them (APP 12); (b) request correction (APP 13); and (c) make a complaint about a breach of the APPs to Company in the first instance and, if unresolved, to the Office of the Australian Information Commissioner (OAIC).

9.5 Exercising rights

To exercise any right described in this Section 9, contact contact@adhdinbiz.com. Company will respond within the timeframes required by applicable law (generally 30 days for the GDPR; 45 days for CCPA/CPRA, extendable by an additional 45 days in defined circumstances). Company may require verification of the data subject's identity before responding to certain requests.

For opt-out of "sale" or "sharing" under CCPA/CPRA, data subjects may submit a request to contact@adhdinbiz.com with the subject line "Do Not Sell or Share My Personal Information." Company also honours the Global Privacy Control (GPC) browser signal where it is technically feasible to do so.

9.6 Authorised agents

A data subject may designate an authorised agent to exercise rights on their behalf. Company may require written verification of the agent's authority and the data subject's identity.

9.7 No discrimination

Company will not deny services, charge a different price, or provide a different level of service in retaliation for a data subject exercising any privacy right.

10. COOKIES AND SIMILAR TECHNOLOGIES

The Website uses cookies and similar technologies (web beacons, pixels, local storage) for the following purposes:

- (a) **Strictly necessary cookies:** Required to operate the Website (e.g., session, security, load-balancing). These cannot be disabled without rendering parts of the Website inoperative.
- (b) **Functional cookies:** Remember user preferences (e.g., language, region).
- (c) **Analytics cookies:** Measure Website performance and improve content. The Website uses Google Analytics, which sets cookies including `_ga`, `_gid`, `_gat`, and property-specific `_ga_*` cookies. These cookies collect information about how visitors use the Website (pages visited, time on page, referral source) in aggregate form.
- (d) **Marketing and advertising cookies:** Track engagement with Company advertising and enable retargeting and conversion measurement. The Website uses

Meta (Facebook / Instagram) Pixel (cookies including `_fbp` and `fr`); Google Ads (cookies including `_gcl_au`, `IDE`, `NID`, and `DSID`); and TikTok Pixel (cookies including `_ttp` and `tt_appInfo`). Additional cookies may be set by the Website hosting providers (Wix, Go High Level) for session management, security, and load balancing; these are strictly necessary cookies under (a) above.

Where required by applicable law (including the EU ePrivacy Directive and UK PECR), Company will obtain consent for non-essential cookies through a cookie-consent banner before placing them. Data subjects may withdraw consent at any time through the cookie-consent management interface accessible from the Website footer.

11. SECURITY

Company implements technical and organisational measures designed to protect personal data against unauthorised access, alteration, disclosure, or destruction, including:

- (a) Access controls and least-privilege provisioning;
- (b) Encryption in transit (TLS) for Website traffic and platform communications;
- (c) Service-provider due diligence and data-processing agreements;
- (d) Incident-response procedures.

No system can be guaranteed to be 100% secure. Company undertakes to notify affected data subjects and competent supervisory authorities of personal data breaches in accordance with applicable law (including, where applicable, within 72 hours under Article 33 of the EU/UK GDPR).

12. CHILDREN

The Website and Services are intended for adult business operators. Company does not knowingly collect personal information from individuals under the age of 18. If Company becomes aware that personal information of a person under 18 has been collected without verifiable parental consent, Company will delete that information.

13. THIRD-PARTY LINKS

The Website may contain links to third-party websites and services. Company is not responsible for the privacy practices of third parties. Data subjects are encouraged to review the privacy policies of any third-party site or service before providing personal data to it.

14. CHANGES TO THIS POLICY

Company may update this Privacy Policy from time to time. Material changes will be communicated by: (a) posting the updated Policy on the Website; (b) updating the "Last updated" date; and (c) for active Clients, providing reasonable advance notice by email of changes that materially affect data subject rights or processing activities.

Continued use of the Website or Services after the effective date of an updated Policy constitutes acceptance of the updated Policy, except where consent is required by applicable law for new processing activities, in which case Company will obtain renewed consent.

15. CONTACT

For questions about this Privacy Policy or to exercise any right described herein:

Email: contact@adhdinbiz.com

Postal: ADHD Entrepreneur Ventures LLC, 701 Tillery Street Unit 12 Suite 3474, Austin, TX 78702, United States of America

Company does not currently maintain a dedicated EU/UK Article 27 representative. EU/UK data subjects should direct inquiries to contact@adhdinbiz.com.

16. SUPERVISORY AUTHORITIES

Data subjects who are not satisfied with Company's response to a privacy concern may lodge a complaint with the relevant supervisory authority:

- **EU/EEA:** the data protection authority of the data subject's Member State of habitual residence, place of work, or place of the alleged infringement. A list is available at https://edpb.europa.eu/about-edpb/about-edpb/members_en.
- **United Kingdom:** the Information Commissioner's Office at <https://ico.org.uk>.

- **California:** the California Privacy Protection Agency at <https://cppa.ca.gov>.
- **Other U.S. states:** the state Attorney General's office.
- **Australia:** the Office of the Australian Information Commissioner at <https://www.oaic.gov.au>.