

Privacy Policy

ADCO AI LLC respects the privacy of the individuals whose information we handle. This policy explains how ADCO AI LLC and its participating subsidiaries and affiliated entities collect, use, disclose, retain, and protect personal information, and how individuals can exercise their privacy rights.

01 Scope and responsibility

This policy covers adcohq.com and related services that refer to it, business inquiries and communications, recruitment, supplier relationships, and personal information handled in connection with our managed operations and AI services. These services include annotation, evaluation, human review, research, data collection, and quality assurance. Personal information means information that identifies, relates to, or can reasonably be linked to an individual, including personal data under applicable law.

References to "ADCO," "we," "us," and "our" mean ADCO AI LLC and the subsidiaries or affiliated entities involved in the relevant activity. ADCO AI LLC is responsible for the website and business activities for which it determines how and why information is processed. Where another ADCO entity is responsible for an interaction, that entity is identified in the relevant agreement or collection notice. Our privacy contact can help identify and reach the responsible entity.

We act as a controller for information we use for our own business purposes. When we process information on a client's instructions, we act as a processor, service provider, contractor, or subprocessor, as applicable. Section 6 explains this distinction for client services. Additional applicant, workforce, participant, or project notices may provide more specific information. This policy does not limit rights or obligations under applicable law.

02 Personal information we handle

The information we handle depends on the interaction and the services involved. The following categories are not collected from every individual.

Contact and professional information. Names, email addresses, telephone numbers, employer or organization, job title, location, professional profiles, and business website details.

Business and relationship records. Inquiries, service requirements, correspondence, proposals, contracts, billing contacts, transaction records, and records of services requested or provided.

Recruitment and workforce information. Applications, resumes, education and employment history, qualifications, work samples, interview and assessment information, references, availability, and related communications. Identity, eligibility, attendance, and payment information may also be handled where necessary for an employment or contractor relationship, subject to applicable notices and restrictions.

Project and participant information. Text, images, audio, video, recordings, transcripts, language or demographic information, annotations, evaluation responses, and associated metadata, where included in an authorized engagement. These materials and the results derived from them may contain personal information.

Technical, usage, and privacy records. Internet Protocol addresses, browser and device details, referring pages, timestamps, pages or features used, approximate location inferred from an Internet Protocol address, and diagnostic or security logs. We also handle consents, preferences, complaints, privacy requests, verification information, and records needed to manage those requests.

03 Sources of information

We receive information directly through forms, email, applications, interviews, contracts, communications, and participation in authorized projects. Clients may provide information or grant access to systems needed for an engagement. We may also receive relevant information from authorized business contacts, recruiting sources, references, service providers, and professional public sources. Technical information may be generated automatically when our services are used.

Information obtained indirectly is used for a defined and lawful purpose. Public availability does not itself authorize unrestricted collection, disclosure, or AI training. Where required, we provide information about the source, categories, and intended use within the applicable period.

Please provide only information relevant to your inquiry or application. General forms are not intended for passwords, full payment-card details, sensitive identity documents, confidential client records, or proprietary project samples. Where such information is necessary for an authorized relationship, we arrange an appropriate submission process.

04 How we use personal information

We use personal information to assess and respond to inquiries; evaluate and manage engagements; deliver agreed services and support; communicate with clients, suppliers, and other business contacts; recruit and assess candidates; and administer authorized working relationships.

Information submitted through our business-inquiry form is used to assess and respond to that inquiry and, if an engagement follows, to manage the resulting relationship. Application information is used for ADCO recruitment and related administration. Submitting an inquiry or application does not automatically enroll an individual in promotional mailing lists or authorize unrelated data use.

We also use appropriate information to operate and secure our systems, investigate errors or suspected misuse, maintain necessary business and financial records, meet legal obligations, resolve disputes, and establish, exercise, or defend legal claims. Where permitted and consistent with collection notices, we may use information to understand and improve our own services. The separate restrictions on client-data reuse in Section 6 continue to apply.

Optional marketing and communications are subject to the permissions required by law. You can unsubscribe through the message or contact us to object. Necessary contractual, security, and administrative messages may continue. We may retain a limited suppression record to respect your preference.

Before using information for a materially different purpose, we assess whether the proposed use is compatible with the original purpose and provide further notice or obtain additional permission where required.

05 Legal grounds for processing

Where applicable law requires a legal basis, the basis depends on the particular activity and our role.

Contractual necessity. We process information needed to take steps requested before entering into a contract with an individual or to perform that contract. For contacts acting on behalf of a company, legitimate interests may be the appropriate basis instead.

Legitimate interests. These include responding to business inquiries, managing commercial relationships, evaluating candidates, delivering and administering services, securing systems, preventing misuse, maintaining appropriate records, and protecting legal rights. We consider the necessity of the processing and its impact on individuals, and do not rely on this basis where their rights and interests override ours.

Legal obligations. We process information as necessary to meet applicable employment, tax, accounting, regulatory, and other legal requirements.

Consent. We obtain consent for activities that require it, including certain communications, tracking technologies, sensitive-data uses, or participant projects. Consent can be withdrawn without affecting the lawfulness of earlier processing. The relevant notice explains how to withdraw and the consequences, if any.

If information is required by law or necessary for a service, application, or contract, we explain the requirement and the consequences of not providing it at the relevant stage. For client-controlled information, the client determines the underlying purposes and legal basis, and ADCO processes the information within its authorized role.

06 Client information and AI services

Client information is handled for the engagement described in the applicable agreement and documented instructions. The client's privacy notice generally explains its collection and use of that information. This public policy does not replace a data processing agreement, expand the client's instructions, or authorize independent use of client data.

Human review and access. Annotation, evaluation, verification, and quality assurance may require authorized reviewers to see personal information. Our policy limits access to personnel and approved providers who need the information for the engagement, subject to confidentiality and appropriate access restrictions. Client requirements govern permitted tools, processing locations, copying, downloads, and disclosure.

AI tools and secondary use. We do not use client personal information for independent model training, unrelated datasets, advertising, or licensing for our own purposes. Any training or evaluation performed for a client is limited to the agreed project. Our policy prohibits submission of client information to unapproved external AI tools, public services, personal accounts, or unauthorized devices. Approved use requires documented authorization and the applicable confidentiality, data protection, and international-transfer safeguards.

Downstream processing. Providers that process client personal information are subject to the applicable authorization, confidentiality, security, and use restrictions. We do not treat the right to provide a service as permission to combine client personal information with unrelated information for independent purposes.

Client cooperation. We assist with rights requests, relevant incident investigations, deletion or return, and other data protection obligations to the extent required by law and agreement. Necessary information to assess our processing obligations is provided through the applicable due-diligence or contractual process. Where a request concerns information controlled by a client, we refer it to that client rather than independently disclosing its records.

07 Data collection and participant projects

Where ADCO collects recordings, photographs, text contributions, demographic details, or other information directly for a project, the participant receives additional information appropriate to that project before collection. It identifies the responsible entity, categories collected, purposes, relevant AI training or evaluation uses, recipients or recipient categories, retention, and available rights.

Participation in optional collection is voluntary. Required consent and other permissions are obtained for the stated uses; accepting a general website policy is not consent to every future dataset use or distribution. Where a project involves licensing or disclosing identifiable contributions, the project notice explains that use and the applicable choices.

Requests to withdraw consent are assessed against the relevant processing and applicable rights. We explain any lawful limits relating to prior processing or genuinely anonymized results. Sharing information or using it in an AI project does not, by itself, eliminate privacy rights or justify indefinite retention.

Annotations and derived information remain protected where an individual can still be identified. Pseudonymized information is treated as personal information. Where we use genuinely deidentified information, we maintain protections against reidentification and require recipients to preserve that status where legally required. Any legally permitted testing of those protections is limited to assessing their effectiveness.

08 Disclosures and service providers

We disclose personal information only for an authorized purpose, with an appropriate basis and safeguards. Recipient categories include:

Service providers and professional advisers. Providers supporting hosting, databases, authentication, communications, document management, recruitment, security, analytics where used, payment or administrative services, and legal, accounting, or insurance advice. Providers processing information on our behalf are subject to appropriate contractual restrictions on access, use, confidentiality, security, and onward disclosure.

Participating subsidiaries and affiliates. Relevant ADCO entities supporting authorized administration, management, or service delivery. Information sharing is limited to the need arising from the activity; corporate affiliation does not permit unrestricted access or unrelated reuse.

Clients and project recipients. Clients and recipients authorized under an engagement or identified in a participant notice, within the applicable purpose, instructions, permissions, and legal requirements.

Authorities and transaction parties. Recipients required by a valid legal obligation or process, or where a permitted disclosure is necessary to protect rights, safety, or security. Necessary information may also be disclosed in a proposed or completed financing, restructuring, merger, acquisition, or asset transfer, subject to appropriate confidentiality and privacy protections. We assess the lawful scope of requests and give notice where required and permitted.

We may also disclose information at an individual's valid direction or with appropriate consent. Our policy is to limit disclosure to information needed for the relevant purpose.

09 International processing

ADCO operates in the United States and Ethiopia. Information may be accessed, stored, or otherwise processed in those countries and in countries where authorized providers operate. Remote access by an overseas entity may constitute a transfer even when information remains hosted elsewhere. Privacy laws and government-access protections can differ between countries.

Where a transfer is restricted by applicable law, we require a permitted transfer mechanism and any necessary additional safeguards before it occurs. Depending on the circumstances, these may include an applicable adequacy decision, approved contractual clauses, a UK transfer agreement or addendum, and required assessments or supplementary protections. Use of the website is not consent to an otherwise restricted transfer.

Client restrictions on countries, hosting, and access remain applicable. You can contact us for information about the locations and safeguards relevant to your information and request a copy or description of applicable safeguards, subject to lawful redactions.

10 Retention, return, and deletion

We retain personal information for the period needed to fulfill its purpose and meet applicable obligations. We consider the relationship or project, the nature and sensitivity of the information, whether the purpose remains active, contractual instructions, recordkeeping duties, and relevant limitation periods. Potential future usefulness alone is not a basis for indefinite retention.

Inquiries and commercial records. Retention supports resolving the inquiry, administering any resulting relationship, and maintaining necessary business, financial, or legal records. A continuing relationship or legal obligation may justify a different period from a closed inquiry.

Recruitment and personnel records. Retention supports the hiring process and related administrative or legal requirements. Additional consideration for future roles requires a disclosed purpose and valid basis. Employment, contractor, and payment records follow the applicable relationship and statutory requirements.

Client and participant information. Client data follows the agreed retention and return-or-deletion instructions. Direct participant collection follows the period or meaningful criteria disclosed for the project. Security and diagnostic records are kept for a proportionate operational, investigation, or legal need.

When information is no longer needed, our policy requires secure deletion or genuine anonymization. Residual backup copies are restricted from ordinary use and removed through the applicable backup lifecycle. If a backup is restored, applicable deletion instructions are reapplied. A legal hold is limited to the information and period necessary. Contact us for the retention period or criteria relevant to your information.

11 Security and incident response

ADCO uses administrative, technical, organizational, and physical safeguards designed to protect personal information against unauthorized access, loss, misuse, alteration, and disclosure. Safeguards are selected in light of the information, processing risks, environment, and contractual requirements.

Our standards address work-related access, confidentiality, personnel guidance, approved systems, secure handling, and disposal. Authentication, access review, encryption, logging, device restrictions, and physical controls are applied as appropriate to the environment and engagement.

Suspected incidents are assessed for containment, investigation, remediation, and appropriate cooperation with affected clients. Notifications to clients, authorities, and affected individuals are made according to our role and the requirements and deadlines of applicable law and contract. You may report a concern through the contact in Section 18.

No transmission or storage method is completely secure. Please avoid including unnecessary sensitive information in an initial incident report or privacy request.

12 Cookies, advertising, and online choices

Cookies and similar technologies can support website functionality, security, sessions, preferences, and usage measurement. Necessary technologies help the service operate. Where non-essential analytics or other technologies are deployed, additional information and choices are provided as required, including consent before activation where applicable.

You can manage browser storage through browser settings and any controls available on the relevant service. Blocking necessary technologies can affect functionality. Where processing depends on consent, withdrawing it must be as easy as giving it. Contact us for help with your choices or for information about technologies relevant to your interaction.

ADCO does not sell personal information collected through website inquiries or recruitment, or share that information for cross-context behavioral advertising. We do not trade client personal information for our own purposes. Separate participant collection or licensing is governed by the disclosures and permissions described in Section 7.

Browser Do Not Track signals do not have a uniform implementation standard, and our website does not commit to responding to those signals. This is separate from legally recognized opt-out preference signals, such as Global Privacy Control, which we honor when required for the relevant processing. Providers of embedded or linked third-party services may collect information under their own notices, including about activity across services; the particular technologies and permissions determine the collection involved.

13 Privacy rights

Your rights depend on applicable law, your location, the processing, and ADCO's role. Subject to lawful conditions and exceptions, they may include:

Access and transparency. Confirmation of whether information is processed; information about categories, sources, purposes, and recipients; and access to or a copy of personal information.

Correction, deletion, and restriction. Correction of inaccurate information, deletion of information, or restriction of particular processing where the applicable conditions are met.

Portability. Receipt of qualifying information in a structured, commonly used, machine-readable format, and transmission to another controller where required and technically feasible.

Objection and withdrawal. Objection to processing based on legitimate interests on grounds relating to your situation, and withdrawal of consent for future processing. You may object to direct marketing at any time, including related profiling, and we will stop that processing.

Additional choices. Where applicable, opting out of sale, sharing, targeted advertising, or certain profiling; limiting specified uses or disclosures of sensitive information; and safeguards for significant automated decisions. A right may not be relevant where ADCO does not carry out the activity concerned.

We do not unlawfully discriminate or retaliate against individuals for exercising privacy rights. You may also have a right to appeal a refusal or complain directly to a regulator.

14 Requests, verification, and complaints

Send privacy requests to privacy@adcohq.com. Describe your relationship with ADCO and the information or activity concerned so that we can locate the relevant records. We seek only information reasonably necessary to verify identity and authority and manage the request. Do not send a full identity document unless we explain why it is necessary and provide an appropriate channel.

Authorized representatives may act where permitted, subject to appropriate proof of authority and verification. Opt-out requests are handled according to the applicable rules and are not subjected to identity-verification requirements that the law prohibits. We do not require an account solely to submit a privacy request.

We respond within applicable deadlines. Under EU or UK data protection law, the ordinary period is one month, with up to two further months where a permitted extension is necessary and explained within the initial period. Under many U.S. state laws, access, correction, and deletion requests ordinarily receive a response within 45 calendar days; opt-outs may have shorter deadlines. Any extension, fee, or refusal is limited to what the law permits and is explained where required.

Where we process information for a client, we route the request to the responsible client and provide assistance required by law and agreement. To challenge our response, email privacy@adcohq.com with "Privacy Appeal" in the subject line. We review the decision and respond within the applicable period.

You may complain directly to a competent data protection authority, state regulator, attorney general, or other relevant body. Where applicable, this includes a supervisory authority in the European Economic Area or the UK Information Commissioner's Office. Contacting ADCO first is not a condition of exercising a statutory complaint right.

15 Sensitive information and children

General website forms are not intended to collect sensitive personal information. Sensitive information can include health information, government identifiers, protected characteristics, precise location, and biometric information used to identify a person. A photo or voice recording can contain personal information without being used for biometric identification.

Processing sensitive information requires a necessary, authorized purpose and the additional legal conditions and safeguards applicable to that information. Our ordinary inquiry process does not authorize submission of health records, payment-card data, or other regulated datasets. Projects involving such information require separate assessment and appropriate arrangements before processing, including specific agreements where required.

The public website is intended for business and employment-related use and is not directed to children under 13. We do not knowingly collect information from children under 13 through general website forms. If you believe this has happened, contact us so we can investigate and take appropriate action. Any separately authorized project involving minors is subject to applicable age limits, parental or guardian permissions, and additional child-privacy protections.

16 Automated processing

Our services may involve AI-assisted workflows and human evaluation of AI outputs. Where ADCO conducts profiling or makes a solely automated decision with legal or similarly significant effects, the activity is subject to the permitted basis, transparency, and safeguards required by law. Relevant information about the processing and its consequences, and applicable rights to human intervention, to express a view, and to challenge the decision, are provided for that activity.

17 External services and policy changes

Independent websites and services linked from our website have their own privacy practices. Their notices govern their independent processing. ADCO remains responsible for its own disclosures and for obligations arising when it engages a provider to process information on its behalf.

We review this policy as our services, practices, and applicable requirements change. Revisions are made available through our website. Where changes materially affect how we use previously collected information, we provide appropriate notice, such as a prominent website notice or direct communication when required, and obtain additional consent where necessary. A revised policy does not, by itself, authorize an incompatible new use or remove existing rights.

18 Contact

For privacy questions, requests, complaints, incident reports, or assistance identifying the responsible ADCO entity, contact:

ADCO AI LLC

privacy@adcohq.com

www.adcohq.com

This contact point also routes matters involving participating subsidiaries and affiliated entities to the appropriate responsible entity. You may request this policy in an accessible format.