

CLIENT DATA PROTECTION OVERVIEW

ADCO AI LLC

ADCO AI LLC processes personal data for authorized business purposes and applies project-scoped access, confidentiality, security, retention, incident, and deletion controls appropriate to the engagement and applicable written instructions.

1. PROCESSING ROLES AND INSTRUCTIONS

ADCO acts as a processor or subprocessor when it handles personal data on a client's documented instructions. The parties identify their roles, processing purpose, categories of personal data and data subjects, duration, authorized systems, approved work locations, retention requirements, security measures, and contact points in the applicable agreement, statement of work, and data processing addendum.

2. CORE DATA PROTECTION CONTROLS

- purpose limitation and data minimization;
- confidentiality obligations and role-appropriate training for authorized personnel;
- named accounts, multi-factor authentication, least privilege, and timely access revocation;
- encrypted transport, private project storage, approved devices, and restricted transfer channels;
- project-specific service-provider review and materially equivalent contractual protection where required;
- reasonable support for data-subject requests, impact assessments, regulatory consultation, and compliance information; and
- documented incident assessment, client notification, corrective action, return, and deletion.

3. RETENTION, RETURN, AND DELETION

Client data is retained only for the contractually or legally required period. At the end of services, ADCO returns or deletes client data in accordance with the applicable agreement and documents the disposition where required. Data remaining in service-provider backups remains protected from ordinary use and expires according to the applicable backup lifecycle.

4. INTERNATIONAL TRANSFERS

When an engagement involves a restricted international transfer, ADCO and the client document the applicable roles, countries, transfer mechanism, official clauses, supplementary measures, and review triggers. Available mechanisms may include the European Commission Standard Contractual Clauses and the United Kingdom International Data Transfer Addendum or International Data Transfer Agreement, completed for the actual data flow.

5. PERSONAL DATA BREACH RESPONSE

ADCO notifies the client without undue delay after becoming aware of a confirmed personal-data breach involving client personal data. Available information may include the nature of the incident, affected data and individuals, likely consequences, containment, remediation, and contact point. The applicable contract and law determine specific deadlines, responsibilities, and regulatory or individual notification.

6. AUDIT AND ASSURANCE

ADCO provides information reasonably necessary to support proportionate client due diligence. Remote evidence review is preferred before intrusive testing. Any review must protect information concerning other clients, confidential systems, credentials, security, personal information, and business continuity.

7. EUROPEAN UNION AND UNITED KINGDOM ENGAGEMENTS

ADCO maintains contractual and operational materials capable of supporting European Union and United Kingdom data-processing engagements. This statement is not a GDPR certification, adequacy decision, or legal opinion. The correct terms and safeguards must be activated for the actual client, roles, data, systems, and transfer.

8. HEALTH INFORMATION

ADCO does not accept protected health information by default. Processing may begin only after a client-specific applicability assessment, executed Business Associate Agreement where required, verified systems and vendor arrangements, risk analysis, minimum-necessary access design, workforce authorization, contingency controls, and written activation approval. ADCO does not claim an official HIPAA certification.

9. PAYMENT DATA

ADCO does not authorize full payment-card numbers, card verification codes, personal identification numbers, or magnetic-stripe equivalents to be entered into its portal, public forms, email, chat, or files. If card payment is offered, card entry must occur through an approved hosted payment provider.

10. CERTIFICATION STATUS

ADCO does not currently claim SOC 2 or ISO/IEC 27001 certification. Representations are limited to implemented controls, contractual commitments, and engagement evidence actually in place.

11. CONTACT

Privacy and data-protection inquiries may be submitted through the contact form at adcohq.com.