Privacy Policy

Daedalus AI Holdings LLC, an Illinois limited liability company with its principal place of business at 1919 West Greenleaf, Chicago, Illinois 60626 ("Daedalus," "we," "us," or "our"), is committed to maintaining the confidentiality, integrity, availability, and lawful processing of personal information. This Privacy Policy describes how Daedalus collects, uses, discloses, safeguards, transfers, retains, and otherwise processes personal information in connection with its website, enterprise software platform, APIs, managed services, private model hosting environments, on-premise deployments, and related offerings (collectively, the "Services").

This Privacy Policy may be incorporated by reference into the Master Services Agreement ("MSA"), Order Forms, Data Processing Addendum ("DPA"), Security Addendum, and related agreements between Daedalus and its customers. In the event of a conflict between this Privacy Policy and a separately executed DPA governing Customer Data, the DPA shall control with respect to such Customer Data.

1. Scope of Application and Roles of the Parties

This Privacy Policy applies to personal information processed by Daedalus when Daedalus acts as a data controller (or business under applicable U.S. privacy laws), including information relating to website visitors, prospective customers, representatives of customers, authorized users of the Services, vendors, and business contacts.

When Daedalus processes personal information contained within Customer Data submitted to the Services, Daedalus acts solely as a data processor or service provider on behalf of the customer pursuant to the MSA and DPA. In such circumstances, the customer determines the purposes and means of processing, and the customer's privacy notice governs the processing of that Customer Data.

Daedalus provides Services exclusively for enterprise and institutional use. The Services are not directed to individuals under eighteen (18) years of age, and Daedalus does not knowingly collect personal information from minors.

2. Categories of Personal Information Processed

Daedalus may collect and process personal information necessary to operate its business and deliver the Services. This may include professional contact information such as name, business email address, business telephone number, job title, employer, and related identifiers necessary to establish and manage contractual relationships.

Daedalus may process account authentication information, including usernames, encrypted or hashed credentials, access roles, account identifiers, and related metadata necessary to manage secure access to the Services.

Technical and usage information may be collected automatically when individuals access the Services or Daedalus' website. Such information may include Internet Protocol (IP) addresses, device identifiers, browser type, operating system, timestamps, session data, authentication logs, API request logs, and system event records. This information is processed for system

security, fraud prevention, operational integrity, service diagnostics, and performance optimization.

Daedalus may also process information provided through support inquiries, contractual communications, compliance reviews, vendor onboarding, or other business correspondence.

When acting as a processor, Daedalus may process personal information included within Customer Data submitted by customers. Such processing occurs strictly under customer instructions and contractual controls. Daedalus does not intentionally solicit sensitive personal information such as government-issued identification numbers, financial account numbers, health records, biometric identifiers, or similar regulated data unless expressly authorized in writing and governed by a contractual framework that addresses such data.

3. Purposes of Processing

Daedalus processes personal information for legitimate and contractually necessary purposes, including the provision, maintenance, and security of the Services; authentication of authorized users; administration of customer accounts; detection and prevention of fraud and abuse; performance of contractual obligations; regulatory compliance; enforcement of contractual rights; protection of Daedalus' rights and property; and communication with customers and business partners.

Personal information may also be processed for internal analytics, service reliability improvements, system optimization, and risk management activities. Where analytics are conducted, Daedalus endeavors to use aggregated or de-identified information where reasonably feasible.

Daedalus does not sell personal information. Daedalus does not share personal information for cross-context behavioral advertising. Personal information and Customer Data are not used to train machine learning or artificial intelligence models.

4. Legal Bases for Processing

Where the General Data Protection Regulation (EU) 2016/679 ("GDPR"), UK GDPR, or other applicable international data protection laws apply, Daedalus processes personal data on lawful bases that may include performance of a contract, compliance with legal obligations, legitimate interests, and consent where required. Where required under GDPR or UK GDPR, Daedalus may appoint a Data Protection Officer or representative as required by law.

Legitimate interests pursued by Daedalus include maintaining service security, preventing fraud, improving product reliability, and managing customer relationships. Such interests are balanced against the rights and freedoms of data subjects.

5. Disclosure and Sharing of Personal Information

Daedalus may disclose personal information to third-party service providers and subprocessors that assist in delivering infrastructure hosting, cloud services, analytics, monitoring, customer support, and related operational functions. Such third parties are bound by written agreements imposing confidentiality, data protection, and security obligations consistent with applicable law and Daedalus' contractual commitments.

Personal information may also be disclosed where required by law, court order, subpoena, regulatory authority, or lawful governmental request. Daedalus may disclose information when necessary to protect the security and integrity of the Services, to enforce agreements, or to protect the rights, safety, and property of Daedalus, its customers, or others.

In the event of a merger, acquisition, reorganization, financing, or sale of assets, personal information may be transferred subject to confidentiality protections and applicable legal requirements.

Daedalus does not sell personal information and does not disclose personal information for monetary or other valuable consideration.

6. Financial Institution and Regulated Entity Considerations

Daedalus provides Services to regulated institutions, including financial institutions subject to the Gramm-Leach-Bliley Act ("GLBA"), healthcare entities, and government agencies. Where applicable, Daedalus processes nonpublic personal information solely in accordance with written agreements and regulatory requirements consistent with the requirements of the GLBA Safeguards Rule (16 CFR Part 314).

Daedalus does not independently access, use, or disclose nonpublic personal information of financial institution customers except as necessary to provide contracted Services and subject to strict confidentiality, security, and contractual controls. Daedalus maintains safeguards designed to protect customer information consistent with applicable regulatory expectations, including administrative, technical, and physical protections.

7. International Data Transfers

Daedalus is headquartered in the United States and may process personal information in the United States or other jurisdictions where Daedalus or its subprocessors operate. Where required by applicable law, Daedalus implements appropriate safeguards for cross-border transfers, including the use of Standard Contractual Clauses or other legally recognized transfer mechanisms.

8. Data Retention

Daedalus retains personal information only for as long as necessary to fulfill the purposes described in this Privacy Policy, to comply with contractual obligations, to satisfy legal and regulatory requirements, or to resolve disputes and enforce agreements.

Customer Data processed under the MSA is retained for the duration specified in the applicable Order Form or project engagement and deleted in accordance with contractual requirements and applicable law. Unless expressly agreed otherwise, Daedalus does not provide long-term archival storage of Customer Data.

9. Security Safeguards

Daedalus maintains administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, use, alteration, disclosure, and destruction. Such safeguards include encryption in transit using TLS 1.2 or higher, encryption at rest using AES-256 or equivalent standards, role-based access controls, least-privilege access principles, system logging and monitoring, secure software development lifecycle practices, vulnerability management procedures, and documented incident response protocols.

While Daedalus employs commercially reasonable security measures aligned with enterprise and financial institution expectations, no system can guarantee absolute security.

10. Individual Rights

Subject to applicable law, individuals may have rights to request access to their personal information, request correction of inaccurate data, request deletion of personal information, restrict or object to certain processing, request data portability, and withdraw consent where processing is based on consent.

Requests may be submitted to legal@trydaedalus.ai. Where Daedalus acts as a processor on behalf of a customer, requests will be directed to the relevant customer for handling in accordance with the governing agreement. Daedalus will respond to verified requests within the timeframes required by Applicable Law and may require reasonable verification of identity prior to fulfilling such requests.

11. U.S. State Privacy Disclosures

To the extent applicable under California and other U.S. state privacy laws, Daedalus acts as a service provider or processor with respect to Customer Data. Daedalus does not sell personal information or share personal information for cross-context behavioral advertising. Daedalus will not discriminate against individuals for exercising privacy rights afforded under applicable law. Daedalus does not respond to “Do Not Track” browser signals except as required under applicable state privacy laws.

12. Children’s Privacy

The Services are intended for enterprise use only and are not directed to children. Daedalus does not knowingly collect personal information from individuals under the age of eighteen (18). If Daedalus becomes aware that it has inadvertently collected such information, it will take reasonable steps to delete it.

13. Updates to This Privacy Policy

Daedalus may update this Privacy Policy from time to time to reflect changes in legal requirements, business practices, or Services. Updated versions will be posted with a revised “Last Updated” date. Where required by law, Daedalus will provide appropriate notice of material changes.

14. Cookies and Online Tracking.

Daedalus' website may use cookies and similar technologies to enable core site functionality, improve user experience, and support security and analytics. Cookies used are limited to those necessary for operational integrity, performance analysis, and service optimization. Daedalus does not use cookies for cross-context behavioral advertising and does not sell personal information. Individuals may manage cookie preferences through browser settings where applicable.

15. Contact Information

Questions regarding this Privacy Policy or Daedalus' privacy practices may be directed to:

Daedalus AI Holdings LLC
1919 West Greenleaf
Chicago, Illinois 60626
Email: legla@trydaedalus.ai

Effective Date: January 1, 2026
Last Updated: March 2, 2026