SynthAI Data Privacy Policy

Introduction

SynthAI (the "Company") is committed to protecting the privacy and security of the data entrusted to us by our clients. This Data Privacy Policy outlines our approach to collecting, processing, storing, and protecting personal and confidential data.

Scope

This policy applies to all SynthAI employees, contractors, and partners who handle or have access to client data. It also applies to all systems, applications, and services provided by SynthAI.

Definitions

- Personal Data: Any information relating to an identified or identifiable individual, such as names, addresses, email addresses, and phone numbers.
- Confidential Data: Any sensitive or proprietary information shared with SynthAI by our clients, including financial data, business strategies, and trade secrets.
- Client Data: Any data provided to SynthAI by our clients, including personal data and confidential data.
- LLM Data: Any data processed or generated by OpenAI's Large Language Model (LLM) API, including text outputs, embeddings, and other model outputs.

Data Collection and Processing

- SynthAI only collects and processes client data that is necessary for the provision of our services.
- We use secure protocols to collect and transmit client data, including encryption and secure APIs.
- Client data is processed in accordance with the instructions of our clients and as required by law.
- We use OpenAI's LLM API to process and analyze client data, and we comply with OpenAI's terms of service and privacy policy.

Data Storage and Security

- SynthAI stores client data in Amazon Web Services (AWS) S3 buckets, which are encrypted using AWS SSE-S3 with AES-256 encryption.
- Data can be stored either in the United States or in Europe depending on the client's request.
- We use AWS Identity and Access Management (IAM) to control access to client data, with role-based access control and multi-factor authentication.
- Client data is backed up regularly, with backups stored in AWS S3 buckets with the same encryption and access controls as the primary storage.
- We implement robust security measures to protect against unauthorized access, disclosure, or loss of client data, including:
    - Firewalls and intrusion detection systems
    - Regular security audits and penetration testing
    - Access controls, including multi-factor authentication and role-based access

Risk Management

- We conduct regular risk assessments to identify, assess, and mitigate risks to client data.
- We implement risk mitigation measures, including encryption, access controls, and secure protocols.

Asset Management

- We maintain an inventory of assets that store, process, or transmit client data.
- We classify assets based on their level of risk and implement appropriate security controls.

Human Resources Security

- We conduct thorough background checks on employees and contractors with access to client data.

- We provide regular training and awareness programs for employees and contractors on data privacy and security best practices.

Supplier Relationships

- We conduct due diligence on suppliers and partners to ensure they meet our data privacy and security requirements.
- We include contractual provisions that require suppliers and partners to comply with our data privacy and security policies.

Incident Response

- We have an incident response plan in place to respond to data breaches and other security incidents.
- We will notify our clients and the relevant authorities in the event of a data breach, as required by law.

Continuous Monitoring and Improvement

- We conduct regular security audits and penetration testing to identify vulnerabilities and improve our security posture.
- We review and update our data privacy and security policies regularly to ensure they remain effective and compliant with applicable laws and regulations.

Training and Awareness

- We provide regular training and awareness programs for employees and contractors on data privacy and security best practices.
- We ensure that employees and contractors understand their roles and responsibilities in protecting client data.

Compliance

- We comply with applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).
- We have designated a dedicated person who oversees our data privacy program.

Changes to this Policy

- SynthAI reserves the right to update this policy from time to time to reflect changes in our services, applicable laws, and industry best practices.
- We will notify our clients of any material changes to this policy.

Contact Us

If you have any questions or concerns about this policy, please contact our CTO at adam.rida@synthai.app

Acknowledgement

By using our services, our clients acknowledge that they have read, understood, and agree to the terms of this Data Privacy Policy.

Effective Date

This policy is effective as of 1 June 2024 and supersedes all prior versions.