PRIVACY POLICY

Effective Date: October 9, 2024

Introduction
At Bespoke Tech LLC ("Bespoke," "we," "us," or "our"), we prioritize your privacy and are dedicated to maintaining the highest standards of data protection and confidentiality. This Privacy Policy outlines the types of personal and sensitive information we collect when you use our AI-powered investment management platform and services. It further explains how we collect, process, disclose, and protect that information. As our Services evolve, we remain committed to updating this Privacy Policy to reflect the latest practices, ensuring compliance with applicable regulations and maintaining transparency with our Users.

Scope of This Policy
This Privacy Policy applies to all users ("Users") of Bespoke's platform, applications, websites, and related services ("Services"). It governs the collection, use, processing, and protection of personal and sensitive data shared by financial institutions, investment professionals, and their clients. This Policy is intended to provide clarity on how we handle your data and to reaffirm our commitment to complying with global data protection regulations, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Information We Collect
We may collect and process the following types of information:

- Personal Information: Names, email addresses, phone numbers, professional titles, and other contact details necessary for account management, authentication, and communication.
- Client Financial Data: Sensitive financial information, such as portfolio details, transaction histories, and performance data, used to provide customized investment insights and services.
- Technical Information: IP addresses, device information, and log data collected through cookies and similar technologies to enhance and secure our Services.
- Usage Data: Information about Users' interactions with our platform, enabling us to personalize experiences and continuously improve the functionality and effectiveness of our offerings.

How We Use Information
First, Bespoke will never use your private or sensitive data, including financial information or uploaded documents, to train models or for any purpose unrelated to your specific use case. Your data remains completely isolated and protected, aligning with our commitment to maintain full user confidentiality.

We use information exclusively to provide and enhance our services while maintaining full compliance with data protection regulations. Specifically, we use information for the following purposes:

- Service Delivery: To provide, personalize, and enhance our investment management services, ensuring that Users receive tailored insights and solutions aligned with their needs.
- Regulatory Compliance: To fulfill legal and regulatory requirements applicable to financial institutions and investment professionals, ensuring adherence to industry standards for data protection.
- Security: To protect against and respond to security threats, including unauthorized access, breaches, and other malicious activities.
- Communication: To send essential communications, updates, security alerts, and other service-related information.
- Service Management: To provide, administer, maintain, and analyze the Services to ensure optimal performance and user experience.
- Research and Development: To improve our Services, conduct internal research, and develop new programs and features without using any user-specific or identifiable data.

Commitment to Data Privacy: At Bespoke, we maintain strict boundaries to safeguard user information. We adhere to a policy of data separation, ensuring that no private user data, financial information, or uploaded content is used in the development, training, or refinement of our AI models. We maintain rigid and impenetrable data walls,

guaranteeing that all sensitive and financial information remains confidential and isolated from any AI development processes. Bespoke's approach aligns with industry standards for financial technology firms, ensuring complete user privacy and compliance with regulatory requirements.

Aggregated or De-Identified Information: We may aggregate or de-identify personal information in a way that it cannot be used to identify individual users. We use this anonymized data to analyze the effectiveness of our Services, add features, conduct research, and improve our offerings. Aggregated data, such as general user statistics, may be shared with third parties, published, or made available in general reports. This data remains in a de-identified state, and we do not attempt to re-identify it unless required by law.

Data Usage Limitations: Bespoke will never use your private or sensitive data, including financial information or uploaded documents, to train models or for any purpose unrelated to your specific use case. Your data remains completely isolated and protected, aligning with our commitment to maintain full user confidentiality.

Retrieval-Augmented Generation (RAG) System and Sensitive Data Handling
Our RAG system is designed to retrieve and process relevant information securely and efficiently. When handling sensitive data, we implement stringent controls and adhere to the following practices:

- Temporary Data Storage: The RAG system retrieves relevant information from secure, external knowledge bases and processes it temporarily. Sensitive data is stored only in memory during the response generation process.
- Immediate Deletion: After generating a response, all sensitive data accessed by the RAG system is immediately cleared from memory. Any temporary files or cached information created during processing are deleted without delay.
- Secure Data Handling: We use encryption protocols (e.g., AES-256) to secure data at rest and in transit. Access to sensitive information is restricted through strict access controls and secure memory management techniques.

Third-Party Integration for RAG
When leveraging third-party services, often Amazon Web Services (AWS) to support our RAG system:

- Short Retention Policies: We configure short retention periods for any temporary storage or logs generated during the RAG process, ensuring sensitive data is not retained longer than necessary.
- Automated Deletion: We use Amazon S3's lifecycle policies and AWS Key Management Service (KMS) to automate and secure data deletion, ensuring data is inaccessible once it is no longer needed.
- Compliance and Auditing: We monitor data access and deletion activities through AWS CloudTrail, providing transparency and traceability for compliance.

Data Security Measures
Bespoke employs a comprehensive, multi-layered approach to safeguard your data, ensuring the highest level of security and compliance. Our protocols include:

- Advanced Encryption: All sensitive and personal data is encrypted using industry-standard AES-256 encryption, both at rest and in transit. We also implement Transport Layer Security (TLS) to secure communications and prevent interception during data transmission.
- Network Security: We use secure firewall configurations, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and block unauthorized access to our networks. Our system architecture is segmented to isolate sensitive data and minimize access points.
- Access Controls and Monitoring: We implement strict role-based access controls (RBAC), ensuring that only authorized personnel with a legitimate business need can access sensitive information. We enforce multi-factor authentication (MFA) for all users accessing our systems, and we log and monitor all access attempts in real-time for suspicious activity.
- Periodic Security Audits and Penetration Testing: We conduct regular internal and external security audits, vulnerability scans, and penetration tests to identify and remediate potential vulnerabilities. Independent

third-party security firms audit our systems annually to ensure compliance with leading standards like ISO 27001 and SOC 2.

- Encryption Key Management: We use AWS Key Management Service (KMS) for secure management of encryption keys. Keys are rotated regularly, and access is restricted to authorized personnel only. We enforce stringent key lifecycle policies, ensuring that keys are destroyed or securely archived when no longer needed.
- Incident Response Plan: We employ real-time monitoring, logging, and reporting mechanisms, enabling us to contain, investigate, and mitigate incidents effectively. Post-incident, we conduct a thorough review and implement improvements to strengthen our security posture.

Data Retention and Deletion

Bespoke adheres to industry-standard data retention and deletion practices, ensuring that sensitive information is stored only as long as necessary and securely deleted thereafter. Our data lifecycle management strategies align with the standards established by industry leaders, and include:

- Retention Policies: We maintain strict data retention policies that define the duration for which various categories of data are retained. For example:
    - Temporary and Transient Data: Data accessed or processed temporarily through our RAG system is immediately deleted upon completion of the task, ensuring that sensitive data is not stored beyond its immediate use.
    - Client Financial Data: Retained only as long as necessary to fulfill user requirements and comply with legal, regulatory, or contractual obligations.
    - Usage Logs: Retained for up to one year for security and analytics purposes, after which they are securely deleted or anonymized.
- Automated Data Deletion Protocols: We use AWS S3's lifecycle policies and AWS Backup tools to automate the deletion of data according to our retention schedules. This includes deleting logs, snapshots, and other temporary data stored in AWS environments.
- Secure Deletion Procedures: For data requiring secure deletion, such as client financial records or sensitive information, we use methods that adhere to secure data erasure standards:
    - Data Overwriting: Data is overwritten with random values multiple times before deletion to ensure it is irretrievable.
    - Key Destruction: We use AWS KMS to manage encryption keys. When data is no longer needed, the associated encryption keys are securely destroyed, rendering the data inaccessible.
- Data Deletion Monitoring and Auditing: Our systems log and monitor all deletion activities. We conduct periodic audits of our deletion practices to ensure compliance and verify that data has been properly erased from our systems.
- Data Minimization: We minimize the collection and storage of sensitive data wherever possible, only retaining the minimum amount necessary for legitimate business purposes. This reduces risk and limits the volume of data needing management and deletion.
- Regular Policy Reviews: We review and update our data retention and deletion policies regularly to align with evolving regulations and industry best practices. We ensure that all changes are reflected in our systems and communicated clearly to Users.

By implementing these comprehensive data security and lifecycle management measures, Bespoke ensures that sensitive information is protected, used appropriately, and securely deleted when no longer needed. Our practices demonstrate our commitment to maintaining the highest standards of data integrity and user trust.

Data Subject Rights

Depending on your location and the data protection regulations applicable to you, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), you may have several rights concerning your personal information. We are committed to upholding these rights and ensuring that you have control over your data. Your rights may include:

Right to Access: The right to request access to the personal information we hold about you, including details about how we use and process your data.

Right to Rectification: The right to request that we correct any inaccuracies or incomplete information related to your personal data.
Right to Erasure (Right to be Forgotten): The right to request deletion of your personal information from our records, subject to legal and regulatory requirements that may mandate its retention.
Right to Restrict Processing: The right to request a restriction on how we process your data, particularly if you contest its accuracy or object to our processing activities.
Right to Data Portability: The right to receive a copy of your personal data in a structured, commonly used, and machine-readable format and to transfer that data to another controller where technically feasible.
Right to Object: The right to object to the processing of your personal data, including for direct marketing purposes or when processing is based on legitimate interests.
Right to Withdraw Consent: If we process your personal information based on your consent, you have the right to withdraw your consent at any time. This will not affect the lawfulness of processing based on consent before its withdrawal.
Right to Lodge a Complaint: The right to lodge a complaint with your local data protection authority if you have concerns about how we manage your personal information.

To exercise any of these rights, please contact us your account representative. We will respond to your request in accordance with applicable laws and aim to address your concerns in a timely manner.

Transferring Personal Data to the United States
Bespoke is headquartered in the United States. As part of our service delivery, the personal information we collect from you may be processed in the United States. By using Bespoke's services, you acknowledge and agree that your personal information will be processed in the United States. The United States does not have an "adequacy" decision from the European Union under Article 45 of the General Data Protection Regulation (GDPR). To ensure appropriate safeguards, pursuant to Article 46 of the GDPR, Bespoke has implemented binding, standard data protection clauses that are enforceable by data subjects in the European Economic Area (EEA) and the UK. These clauses are enhanced in accordance with guidance from the European Data Protection Board and will be updated as necessary to align with the latest regulatory standards.

Depending on the circumstance, Bespoke may also collect and transfer personal data to the United States based on:

- Your explicit consent,
- The necessity to perform a contract with you, or
- The need to fulfill a compelling legitimate interest of Bespoke, in a manner that respects and does not infringe upon your rights and freedoms.

Bespoke is committed to applying appropriate safeguards to protect the privacy and security of your personal data. We only use your data in accordance with our relationship with you and in compliance with the practices outlined in this Privacy Policy. Bespoke also enters into data processing agreements and utilizes standard contractual clauses with third-party vendors whenever feasible and appropriate, ensuring compliance and the highest level of data protection.

Children's Privacy
Our Services are intended for professional use and are not directed at children under the age of 18. We do not knowingly collect information from children. If we become aware that a child's information has been collected, we will promptly delete it.

Updates to This Policy
We may update this Privacy Policy to reflect changes in our practices, technology, or legal obligations. We will notify you of material changes through email or in-product notifications. Your continued use of our Services after updates indicates your acceptance of the revised Privacy Policy.

Dispute Resolution
If you have concerns about our handling of your personal information, we encourage you to contact us directly to resolve the matter. We are committed to working with you in good faith to achieve a fair resolution. However, if a

satisfactory outcome cannot be reached, you may have the right to seek recourse through arbitration or lodge a complaint with the appropriate data protection authority in your jurisdiction.

Contact Information
If you have questions or concerns about this Privacy Policy or our privacy practices, please contact us

Bespoke Tech LLC
101 Avenues of the Americas, Suite 900, New York, NY 10013
Email: privacy@bespke.co

Additionally, if you are located within the European Economic Area (EEA) or the United Kingdom (UK), you may contact your local data protection authority or the European Data Protection Supervisor if you have concerns that we cannot address satisfactorily.