PRIVACY POLICY

Last updated: June 10, 2025

Welcome to **SayNotes**. This Privacy Policy explains how we collect, use, disclose, and safeguard your personal data when you use the SayNotes mobile application and related services (collectively, the “Service”).

SayNotes is operated by K.I.A.B INVESTMENT MANAGEMENT CONSULTING LTD, a limited liability company incorporated under the laws of the Republic of Cyprus with company registration number HE 421805 ("Company," "we," "us," or "our"), and processes personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (“GDPR”), the California Consumer Privacy Act (“CCPA”), and other applicable privacy laws.

We encourage you to review this Privacy Policy thoroughly to understand your rights regarding your personal data. If you do not agree with our policies and practices, please do not use the Service. For any questions or concerns, you can contact us at support@saynotes.ai.

1. Data Controller

The data controller is: K.I.A.B INVESTMENT MANAGEMENT CONSULTING LTD
Email: support@saynotes.ai

2. Information We Collect

We may collect the following categories of data:

- Account Information: Email address, Apple ID or Google ID, authentication tokens.
- Audio Content: Voice recordings, transcriptions, summaries, metadata about the recording (e.g., duration, timestamp.
- Device Data: IP address, device type, OS version, crash logs, app version.
- Usage Data: Interaction logs, feature usage statistics.
- Communications: Support requests, feedback, and opt-in marketing preferences.

3. How We Use Your Data

We process your data to:

- Provide, operate, and maintain the Service
- Authenticate users and manage accounts
- Transcribe and summarize voice recordings
- Respond to user requests and provide support
- Improve service quality through analytics
- Send service-related notifications and updates
- Ensure legal compliance

We process your personal data only where we have a legal basis under GDPR or other applicable laws, such as your consent, contractual necessity, or our legitimate interests.

Children's Privacy

Our Service is not intended for users under the age of 16. We do not knowingly collect personal data from children. If we become aware of such data, we will delete it.

4. Data Sharing

We may share your personal data with select third parties in order to operate, improve, and support the Service, as well as in specific legal or business situations. All third parties are required to process your data in accordance with applicable data protection laws and under contractual obligations to protect your privacy.

4.1 Third-Party Service Providers

We share personal data with trusted service providers to perform essential business functions. These partners include:

- **Firebase (Google LLC):** Data storage, authentication, and real-time databases (Firestore)
- **AssemblyAI:** Audio transcription services
- **OpenAI:** Text summarization, chat features
- **Adjust:** Marketing analytics and attribution tracking
- **Heroku:** Server hosting, queues and database

4.2 Platform-Specific Sharing

- **Apple (iOS):** Certain data may be shared with Apple in accordance with their App Store policies

4.3 Business Transfers

We may disclose or transfer personal data in connection with, or during negotiations of, any merger, acquisition, financing, sale of assets, or transition of service to another provider.

4.4 With Your Consent

We may share your information for other purposes if you provide explicit consent.

4.5 Legal Obligations

We may disclose personal data if required to comply with applicable law, legal requests, court orders, subpoenas, or governmental investigations.

4.6 Vital Interests and Enforcement

We may disclose your data when necessary to protect the vital interests or legal rights of the Company, our users, or others — including investigating fraud, enforcing our Terms of Use, and addressing security concerns.

4.7 Use of Google APIs

We use certain Google APIs, such as Google Sign-In, to support secure account authentication and improve user experience.

In accordance with the Google API Services User Data Policy, we do not use any data obtained through Google Workspace APIs to develop, improve, or train generalized artificial intelligence (AI) or machine learning (ML) models.

All data accessed via Google APIs is handled in accordance with this Privacy Policy and applicable data protection laws, including the GDPR.

5. Legal Bases for Processing Your Personal Data

We process your personal data only when we have a lawful basis to do so, depending on your location and the nature of the processing.

5.1 EU and UK Users

Under the GDPR and UK GDPR, we rely on the following legal bases:

- Consent – When you give clear permission for a specific use (e.g. marketing). You may withdraw consent at any time.
- Contract – When processing is necessary to provide the Service or respond to your requests.
- Legal Obligation – When required to comply with applicable laws.
- Legitimate Interests – When processing supports our business operations and is not overridden by your rights.
- Vital Interests – In rare cases, to protect someone’s life or safety.

5.2 Canada

We rely on:

- Express or Implied Consent – As appropriate under Canadian law.
- Legal Exceptions – For fraud prevention, legal claims, or emergencies.

5.3 United States and Other Regions

We process your information in accordance with applicable local laws and based on:

- Consent
- Contractual Necessity
- Legal Compliance
- Legitimate Business Interests

5.4 Our Global Commitment

Regardless of your location, we:

- Process data lawfully and fairly
- Collect only what we need for specific purposes
- Keep data secure and only as long as necessary

You may have rights to access, correct, delete, or restrict your data. To exercise these, contact us at support@saynotes.ai.

6. International Data Transfers and Storage

6.1 Global Data Storage and Processing

To operate our Services efficiently and reliably for users worldwide, we may store and process your personal data on servers located in various countries, including but not limited to:

- United States
- European Union member states
- United Kingdom
- Canada
- Australia
- Japan

Our primary infrastructure is hosted in the United States, but we rely on cloud services and vendors that may process data internationally, depending on the features and providers involved.

6.2 Legal Safeguards for International Transfers

We implement appropriate safeguards to protect personal data when transferred outside of your country or region of residence. These include:

- Standard Contractual Clauses (SCCs): For data transfers from the European Economic Area (EEA), the UK, or Switzerland to countries without adequate data protection laws, we rely on the European Commission's SCCs to ensure equivalent protection.
- Binding Corporate Rules (BCRs): Where applicable, we follow approved BCRs to enable intra-group data transfers under consistent privacy standards.
- Transfer Impact Assessments: We assess the legal environments of third countries where data may be processed and apply additional safeguards where needed.

6.3 Security Measures

All international transfers are protected through:

- End-to-end encryption during transmission and at rest
- Access controls and authentication protocols
- Vendor audits and contractual data processing agreements

These measures are designed to ensure that your data remains secure, confidential, and processed in accordance with applicable laws.

6.4 Your Rights

You have the right to:

- Request details about where your personal data is stored and processed
- Object to data transfers under certain conditions
- Request that your data be stored within a specific jurisdiction, where technically and legally feasible

To exercise these rights, contact us at support@saynotes.ai.

6.5 Compliance with International Laws

We comply with applicable data protection laws in all jurisdictions where we operate, including but not limited to:

- General Data Protection Regulation (GDPR) – EU/UK
- California Consumer Privacy Act (CCPA) – United States
- Personal Information Protection and Electronic Documents Act (PIPEDA) – Canada
- Privacy Act 1988 – Australia

- Act on the Protection of Personal Information (APPI) – Japan

6.6 Ongoing Review

We regularly update our data handling practices to maintain compliance with global privacy laws and standards. By using our Services, you consent to the transfer, storage, and processing of your information in accordance with this section.

7. Data Retention

7.1 Retention Period

We retain your personal information only for as long as necessary to:

- Provide and maintain our Services
- Comply with legal and regulatory obligations
- Resolve disputes
- Enforce our contractual agreements

We do not keep personal data longer than the duration of your active account unless a longer retention period is required or permitted by law.

7.2 Your Control Over Data

You have full control over the data you upload and store within our Services:

- **Document Deletion:** You may delete your recordings, transcripts, and summaries at any time via the app. Once deleted, this data is permanently removed from our active systems.
- **Account Deletion:** You may delete your entire account, which will result in the irreversible deletion of all associated personal data and user content, unless retention is required by law.

7.3 Deletion and Anonymization

We delete or anonymize personal data when:

- You request deletion
- The data is no longer needed for the purposes outlined in this Privacy Policy
- We have no ongoing legitimate interest to continue processing it

7.4 Data in Backup Systems

In some cases, your information may temporarily remain in encrypted backup archives. In such cases:

- It is securely stored and isolated from routine access
- It is not used for any processing purposes
- It is deleted automatically as part of our regular backup retention schedule

7.5 Legal Obligations

Certain data may be retained if required by:

- Applicable tax, accounting, or legal regulations
- Law enforcement or governmental authorities, under lawful request

In such cases, we retain only what is strictly necessary and implement appropriate safeguards to protect your data.

7.6 Our Commitment to Data Minimization

We are committed to the principles of data minimization and storage limitation. We regularly review our retention policies and delete or anonymize data that is no longer required.

8. How Do We Keep Your Information Safe?

We are committed to protecting your personal information through a combination of technical, organizational, and administrative security measures. Below is an overview of our key practices:

8.1 Data Encryption and Transmission

- All data transmitted between your device and our servers is encrypted using industry-standard SSL/TLS protocols.
- Sensitive user data may be encrypted at rest and in transit to provide an added layer of protection.

8.2 Infrastructure and Storage

- We use Firebase (Google Cloud) to host and manage core backend services. Firebase complies with leading security standards, including ISO 27001 and SOC 2.
- Data is stored in secure, geographically distributed data centers with built-in redundancy and disaster recovery protocols.

8.3 Access Control and Authentication

- Access to personal data is restricted to authorized personnel only.
- Administrative access is protected using strong authentication, including multi-factor authentication (MFA).
- Least privilege principles are applied to all system permissions.

8.4 Monitoring and Incident Response

- We monitor our systems 24/7 for security events and vulnerabilities.
- A formal incident response process is in place to address security threats promptly and transparently.

8.5 Backups and Data Recovery

- Regular, secure backups are maintained to ensure data integrity and continuity.
- Backup data is encrypted and stored separately from live production systems.

8.6 Security Audits and Testing

- Internal audits and code reviews are conducted regularly.
- Independent third-party penetration tests and security assessments are performed periodically.

8.7 Employee Awareness and Training

- All team members receive regular training on data security, privacy obligations, and secure coding practices.
- Access to user data is strictly monitored and logged.

8.8 User Responsibility

While we take extensive steps to safeguard your information, you also play a role in protecting your data. We recommend that you:

- Use a strong and unique password for your account.
- Avoid using public or unsecured networks to access the app.
- Keep your device and operating system updated.
- Enable device-level security features where available.

8.9 No Guarantee of Absolute Security

Although we implement best-in-class security measures, no method of transmission over the Internet or method of electronic storage is completely secure. Therefore, we cannot guarantee absolute security.

If you believe your interaction with us is no longer secure or you become aware of any actual or suspected breach, please contact us immediately at support@saynotes.ai.

9. What Are Your Privacy Rights?

We respect your privacy rights and are committed to enabling you to exercise them in accordance with applicable global data protection laws.

9.1 General Rights for All Users

No matter where you are located, you may have the right to:

- Access the personal information we hold about you.
- Request corrections to inaccurate or incomplete data.
- Delete your account and associated personal information.
- Withdraw consent for data processing (where consent is the legal basis).
- File a complaint regarding our privacy practices.

To exercise any of these rights, please contact us at: support@saynotes.ai.

9.2 Regional-Specific Rights

Depending on your country of residence, additional rights may apply:

European Economic Area (EEA), United Kingdom (UK), and Switzerland

Under the GDPR and UK GDPR, you have the right to:

- Obtain a copy of your personal data (data portability).
- Request correction or deletion of your data.
- Restrict or object to processing.
- Withdraw consent at any time (where processing is based on consent).
- File a complaint with your local data protection authority:
    - EEA & UK Authorities
    - Switzerland - FDPIC

California, USA (CCPA)

If you are a California resident, you may:

- Know what categories of personal data we collect and how it's used.
- Request deletion of your personal information.
- Opt-out of the sale of your personal information (Note: we do not sell data).
- Exercise your rights without discrimination.

Canada (PIPEDA)

Under Canadian law, you may:

- Access your personal data.
- Challenge its accuracy.
- Withdraw consent for certain types of data use.

Australia (Privacy Act 1988)

Australian users may:

- Request access to their personal data.
- Correct inaccurate information.
- Submit complaints regarding privacy handling.

Other Regions

We strive to comply with applicable laws in all jurisdictions. If you have questions about your privacy rights in your country, please contact us directly.

9.3 How to Exercise Your Rights

- Via Account Settings: You can manage most of your personal information directly in your account settings.
- Account Deletion: You may request permanent deletion of your account by contacting us or using in-app options where available.
- Data Retention: Please note we may retain certain information to comply with legal obligations or enforce our Terms of Use.
- Consent Withdrawal: Where processing is based on consent, you may withdraw it at any time. This does not affect data processed prior to withdrawal.

9.4 Response to Requests

We will respond to all data subject requests in accordance with applicable laws. We may require you to verify your identity before completing your request.

9.5 Updates to Privacy Practices

We regularly review and update our privacy practices. Please check this privacy notice periodically for any changes. If you have any questions or concerns about your privacy rights, please contact us at: support@saynotes.ai.

10. CCPA Notice (California Users)

If you are a California resident, you are entitled to specific privacy rights under the **California Consumer Privacy Act (CCPA)** and the **"Shine the Light"** law.

10.1 "Shine the Light" Law (Cal. Civ. Code § 1798.83)

You may request information about personal data we have shared with third parties for direct marketing purposes in the past 12 months. This request is available once per year, free of charge.
To make a request, contact us at: support@saynotes.ai.

10.2 CCPA Privacy Rights

Under the CCPA, California residents have the right to:

- Right to Know
  Request details about personal information collected, including:
  - Categories and specific pieces of personal information
  - Sources of information
  - Purposes of collection
  - Categories of third parties with whom data was shared
  - Any data sold or disclosed for business purposes (we do not sell personal data)
- Right to Delete
  Request deletion of personal information we've collected, subject to legal exceptions.
- Right to Opt-Out
  Opt out of the sale of personal information (Note: we do not sell personal data).
- Right to Non-Discrimination
  Exercise your rights without being denied goods or services, or receiving different prices or service levels.

10.3 Personal Information We Collect

In the last 12 months, we may have collected the following categories of information:

- Personal identifiers (e.g., name, email address)
- Customer records (e.g., account and billing details)
- Protected classification characteristics (e.g., gender, birth year)
- Geolocation data

This information is collected from:

- You directly
- Your devices while using our app
- Authorized third-party service providers

We use this data to deliver, maintain, and improve our services, as outlined in this Privacy Policy.

10.4 How We Share Your Information

We share your personal data with service providers to support our operations (e.g., hosting, analytics, subscriptions).
All such sharing is done under binding contractual agreements that protect your data.
We do not sell your personal information.

10.5 Exercising Your Rights

To submit a CCPA request, you or your authorized agent may:

- Email us at support@saynotes.ai.
- Use the contact information provided at the end of this Privacy Policy

We may request additional information to verify your identity before responding.
We aim to respond within 45 days, with a possible extension of another 45 days, if necessary.

10.6 Verification Process

To protect your information, we may ask for account-related details or identification. We will only use this data to verify your request.

If we cannot verify your identity, we may deny your request.

10.7 Additional Rights for California Minors

If you are under 18, live in California, and have a registered account, you can request removal of any content you have publicly posted.
To do so, email us with:

- Your account email
- A statement that you reside in California

We will remove the content from public view; however, some data may remain in our systems due to technical limitations.

11. Do-Not-Track, App Tracking Transparency, and Analytics

11.1 Do-Not-Track (DNT) for Web Browsers

Some web browsers offer a "Do-Not-Track" (DNT) feature. However, due to the absence of a consistent industry standard, our website does not currently respond to DNT signals.

11.2 App Tracking Transparency for iOS

We comply with Apple's App Tracking Transparency (ATT) framework. Specifically:

- We request your explicit permission before tracking your activity across other companies' apps and websites.
- You can manage tracking permissions at any time through your device settings:
  Settings > Privacy & Security > Tracking
- If you deny tracking, we limit data collection to essential functionality only.

11.3 Analytics and Attribution with Adjust

We use Adjust, a mobile analytics and attribution platform, to help us understand app usage and optimize our services. Adjust may collect data such as:

- Device information (e.g., device model, OS version)
- In-app activity (e.g., screen views, feature usage)
- Installation source and marketing campaign performance

Adjust's data collection on iOS adheres to Apple's ATT requirements. If tracking is disabled, Adjust restricts data collection to non-personalized, aggregated analytics only.
For more information, please refer to Adjust's Privacy Policy.

11.4 Analytics with Amplitude

We use Amplitude, a mobile analytics platform, to anonymously analyze user behavior within our iOS app. This helps us improve product functionality, enhance user experience, and provide more effective technical support.

Amplitude collects only aggregated, non-identifiable data such as:

- Device information (e.g., model, iOS version)
- In-app activity (e.g., screen views, button clicks, feature usage)
- Session duration and engagement patterns

This data is not linked to any real user identity and is used solely for statistical and technical analysis purposes. Amplitude's data collection complies with Apple's App Tracking Transparency (ATT) requirements. If a user declines tracking, data is still collected in a privacy-compliant, anonymized format for essential analytics.

For more information, please refer to Amplitude's Privacy Policy.

11.5 Our Practices

- We use anonymized usage data to improve app performance and user experience.
- Data collection practices are described in Section 2. Information We Collect

11.6 Your Control

- iOS Settings: You can manage app tracking permissions at any time via your device's settings:
  Settings > Privacy & Security > Tracking
- In-App Settings: Where applicable, our app provides controls to manage data collection preferences.
- Contact: For any concerns about data collection or tracking, email us at support@saynotes.ai.

12. Third-Party Links

12.1 Third-Party Websites and Services

Our Service may contain links to websites, online services, or mobile applications operated by third parties. These third-party services are not owned or controlled by us, and their inclusion does not imply our endorsement.

12.2 No Responsibility for Third Parties

- We are not responsible for the content, privacy policies, or practices of any third-party websites or services. Use of any third-party resources is at your own risk.
- We do not guarantee or verify the accuracy, safety, or functionality of third-party content.
- We are not liable for any loss or damage caused by your use of third-party websites, services, or advertisements.
- Any interaction with third-party services, including advertisements, is solely between you and the third party.

12.3 Data Shared with Third Parties

If you choose to access or use third-party services, any data you provide is governed by their own privacy policies and terms. Your data will not be protected under this Privacy Policy.

We strongly recommend that you review the privacy practices of all third-party websites or services before providing any personal information.

12.4 User Responsibility

As a user, you are responsible for:

- Understanding the risks of interacting with third-party content
- Reviewing third-party privacy policies and terms before engaging
- Contacting third parties directly for more information about how they handle your data

13. Changes to This Policy

13.1 Ongoing Updates

We are committed to maintaining transparency about our data practices. We may update this Privacy Policy from time to time to reflect:

- Changes in our business operations
- Compliance with new legal or regulatory requirements
- Improvements to our data protection measures
- Feedback from users

13.2 How We Notify You

When changes are made, we will:

- Update the “Last Updated” date at the top of this Privacy Policy
- Post the revised version within the app and/or on our website

For material changes that significantly impact your rights or our obligations, we may additionally:

- Display a prominent in-app or website notice
- Notify you directly via email or in-app notification
- Request your acknowledgment before continuing use of the Service

13.3 What Constitutes a Material Change

Material changes may include, but are not limited to:

- New categories of personal data being collected
- Expanded purposes for data use or sharing
- Additional third-party disclosures
- Significant updates to security practices

- Alterations in user rights or how they may be exercised

13.4 Your Responsibility

While we aim to communicate all significant updates, we encourage you to:

- Periodically review this Privacy Policy
- Monitor the "Last Updated" date for recent revisions
- Contact us with any questions or concerns about the updates

13.5 Continued Use Indicates Acceptance

By continuing to use our Services after an updated Privacy Policy is posted, you acknowledge and agree to the changes. If you do not agree with the revised terms, you should discontinue use of the Service and contact us to close your account.

If you have questions about changes to this Privacy Policy, please contact us at: support@saynotes.ai

14. How Can You Review, Update, or Delete the Data We Collect From You?

14.1 Your Rights

We respect your right to control your personal information. Depending on your location and applicable laws (such as the GDPR, CCPA, or other data protection frameworks), you may have the right to:

- **Access** – Request a copy of the personal information we hold about you.
- **Update** – Correct or update your personal data if it is inaccurate or incomplete.
- **Delete** – Request deletion of your personal information from our systems.
- **Restrict** – Request that we limit how your personal information is processed.
- **Object** – Object to our use of your data in specific situations.
- **Data Portability** – Request your data in a portable, machine-readable format.

14.2 How to Exercise Your Rights

You can exercise these rights in the following ways:

- **Via Account Settings** – Log into your SayNotes account and manage your privacy and content settings directly.

- **By Email** – Contact us at support@saynotes.ai with a clear description of your request.

14.3 Verification and Timeframes

To protect your information:

- We may require identity verification before processing your request.
- We will respond within the timeframes required by applicable law (typically within 30 days).
- In certain cases, we may not be able to fully comply due to legal obligations or legitimate business interests. If so, we will explain the reason in our response.

14.4 Fees

We do not charge a fee for standard requests. However, we reserve the right to charge a reasonable fee or refuse requests that are manifestly unfounded, excessive, or repetitive.

If you have questions about how we handle your personal data or how to exercise your rights, please contact us at support@saynotes.ai.

15. Contact

If you have questions or requests related to privacy or this Policy, contact us at:
support@saynotes.ai