

Atnias App Privacy Policy

Last updated: **November 23, 2025**

This Privacy Policy describes how Atnias LLC (“Atnias”, “we”, “us”, or “our”) collects, uses, discloses, and protects information when you use our mobile application (the “App”) on iOS and Android.

This Privacy Policy applies only to the Atnias mobile App. It does not apply to third-party websites or services, including Substack, even if we link to them from the App or our website.

By using the App, you acknowledge that you have read and understood this Privacy Policy and agree to the collection and use of information as described herein.

1. Who We Are

The App is provided by:

Atnias LLC, New York, NY, United States
Contact email: support@atnias.com

If you have any questions about this Privacy Policy or our data practices, you may contact us at support@atnias.com.

2. Data We Collect

Atnias is designed to collect only the minimum personal data necessary to operate the App and provide its core functionality.

When you use the App, we may process the following categories of information.

2.1 Account Information

- Email address – used to create and manage your account and to communicate with you about your account (for example, verification and password reset emails).
- Password – used for authentication. Passwords are handled and stored by our backend provider (Appwrite). Passwords are not stored in plain text.

2.2 In-App Preferences

- Likes / favorites – information about which tracks you “like” or mark as favorites. This information is linked to your account so that we can display your liked content in the App.

We do not log or store your detailed listening history (for example, which tracks you played and when) in the current version of the App.

2.3 Technical and Error Information

We use error-reporting tools to identify and analyse crashes and technical issues. In particular, we use Sentry with a configuration intended to minimise personal data:

- Technical information related to crashes and errors (for example, error type, where in the App it occurred, and certain technical context about the App and device environment) may be collected.
- Sentry is configured not to send “default” personally identifiable information, and we do not intentionally attach your email, name, or similar identifiers to error reports.
- Error events may include non-personal metadata such as App area (for example, navigation), operation type, or internal identifiers (for example, track or room IDs) required to diagnose issues.

We do not record or analyse your listening behaviour for marketing, targeting, or recommendation purposes in the current version of the App.

2.4 Subscription and Billing Information

We plan to offer paid subscriptions to unlock additional content and features. When subscriptions are enabled:

- Purchases will be processed by app stores (such as Apple App Store or Google Play Store) and/or a dedicated subscription management provider.
- We do not receive or store your full payment card details.
- We may receive limited information related to your subscription status from these providers (for example, plan type, start and end dates, renewal status), in order to enable or disable premium features in the App.
- For referral programmes, we may store a link between your account and the artist or partner whose referral link you used, in order to calculate revenue sharing in an aggregated manner. We do not disclose your personal identity to artists in this context.

Details of the billing provider and its processing activities will be set out in the provider’s own privacy policy.

3. Data We Do Not Intentionally Collect

In the current version of the App, we:

- Do not collect detailed listening history for analytics or marketing.
- Do not collect product analytics (such as session tracking, funnels, or behavioural analytics) via tools such as Google Analytics, Firebase Analytics, or similar services.
- Do not use advertising identifiers (IDFA/GAID) for advertising or tracking.
- Do not include third-party advertising SDKs or ad networks in the App.
- Do not collect health data or other special categories of personal data.

If these practices change in the future, this Privacy Policy will be updated accordingly and, where required by law, we will seek your consent.

4. How We Use Your Information

We process the information described above for the following purposes:

4.1 Provision and Operation of the App

- Creating and managing user accounts.
- Allowing you to log in securely and use the core features of the App.
- Displaying your liked or favorited content.

- Enabling access to paid features and content for active subscribers.

4.2 Security and Abuse Prevention

- Protecting the App and underlying infrastructure against abuse, fraud, and misuse (for example, bot-like behaviour or attempts to bypass paywalls).
- Detecting, preventing, and responding to unauthorised access to accounts.

4.3 Maintenance, Support, and Improvement

- Monitoring crashes and technical errors using Sentry.
- Analysing technical issues in order to correct faults and improve the stability and performance of the App.

4.4 Communication Related to the App

- Sending essential transactional communications (for example, account verification, password reset, security notices, or important changes to the App or this Privacy Policy).
- Responding to support requests and other communications you send to us.

We do not use your email address collected in connection with the App for promotional marketing campaigns unless you expressly agree to such use in the future.

5. Legal Bases for Processing (EU/EEA and Similar Jurisdictions)

If you are located in the European Economic Area (EEA), the United Kingdom, or another jurisdiction with similar data protection laws, we rely on the following legal bases for processing your personal data:

- Performance of a contract: to create and manage your account and to provide you with access to the App and its core features.
- Legitimate interests: to maintain and improve the App, including security, fraud prevention, and error diagnostics, while appropriately safeguarding your privacy.
- Compliance with legal obligations: to comply with legal, tax, and accounting requirements where applicable.

Where we rely on consent for specific processing activities (for example, certain forms of marketing), we will obtain your consent separately. You may withdraw such consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

6. Sharing of Your Information

We do not sell your personal data.

We may share your information with the following categories of recipients:

6.1 Service Providers

We engage third-party service providers to support the operation of the App and related infrastructure. These providers may process personal data on our behalf and are contractually required to protect it and to use it only in accordance with our instructions. These providers include:

- Appwrite – authentication, account management, and storage of account data (email, password, likes).
- Cloud hosting (AWS) – hosting of audio and visual content. At this stage, user account data is not stored on AWS.
- Sentry – error and crash reporting, configured to minimise personal data.
- Subscription and billing provider (RevenueCat) – management of subscription status and association of store purchases with user accounts.
- Email and communication providers (Resend) – sending of transactional emails (e.g., account verification, password reset), where utilised.

These providers may be located in various jurisdictions. We share only the minimum personal data necessary for them to provide their services.

6.2 Aggregated and Anonymised Data

We may share aggregated and anonymised statistics that do not identify individual users, for example:

- The number of users associated with a particular referral link or artist.
- The number of subscriptions or aggregated revenue associated with a particular artist or partner.

Such aggregated information may be shared with artists, partners, or potential business customers. We do not share identifiable user information, such as email addresses or individual usage profiles, with artists.

6.3 Legal and Compliance Disclosures

We may disclose personal data where we consider it necessary or appropriate to:

- Comply with applicable laws, regulations, or legal processes (e.g., court orders or lawful requests from public authorities).
- Protect the rights, property, or safety of Atnias, our users, or others.
- Detect, prevent, or address fraud, security, or technical issues.

In such cases, we will limit disclosures to what is required under the circumstances and applicable law.

7. International Data Transfers

Our core user account data is stored in the European Union through our backend provider (Appwrite).

Some of our service providers may process data in countries outside your country of residence, including the United States. For example:

- Audio, visual content may be hosted on infrastructure located in the United States (AWS), although user account data is not stored there.

Where personal data is transferred from the EU/EEA/UK to a country that is not subject to an adequacy decision, we implement appropriate safeguards, such as:

- Standard Contractual Clauses approved by the European Commission; and/or

- Other mechanisms recognised under applicable data protection laws.

8. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes described in this Privacy Policy or as required by law.

In particular:

- Account data (email, hashed password, likes): retained for as long as your account is active. If you request deletion of your account, we will delete or anonymise this data, subject to any retention that is legally required. We may delete or anonymise accounts that have been inactive for an extended period (for example, after 24 months of inactivity), in accordance with our internal policies.
- Subscription and billing information: limited subscription-related information may be retained for as long as necessary to comply with accounting, tax, and other legal obligations, which may require retention for several years. Payment card details are not stored by us.
- Technical and error logs: error and crash logs are retained only for as long as needed to diagnose and resolve issues, in line with our and the provider's standard retention periods.

Certain minimal information may be retained in backup copies or logs beyond these periods where required by law or where necessary to establish, exercise, or defend legal claims or to prevent abuse.

9. Your Rights

Depending on your place of residence, you may have some or all of the following rights in relation to your personal data:

- Right of access – to obtain confirmation as to whether we process your personal data and, where applicable, to receive a copy of such data.
- Right to rectification – to request correction of inaccurate or incomplete personal data.
- Right to erasure – to request deletion of your personal data, subject to applicable legal exceptions.
- Right to restriction of processing – to request that we limit the processing of your personal data in specific circumstances.
- Right to data portability – to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller, where applicable.
- Right to object – to object, on grounds relating to your particular situation, to certain processing activities, in particular where we rely on legitimate interests.
- Right to withdraw consent – where processing is based on your consent, to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

If you are a resident of the EEA, the UK, or another jurisdiction with similar data protection laws, you may also have the right to lodge a complaint with your local data protection authority.

To exercise any of these rights, please contact us at support@atnias.com. We will respond within a reasonable time and in accordance with the timeframes required by applicable law. We may need to verify your identity before acting on your request.

10. Children's Privacy

The App is not directed to children under the age of 16, and we do not knowingly collect personal data from children under 16.

We also do not knowingly collect personal data from children under 13. If we become aware that personal data has been collected from a child under 13 without verifiable parental consent, we will take appropriate steps to delete such information.

If you believe that a child has provided us with personal data in breach of this section, please contact us at support@atnias.com.

11. Security

We implement reasonable technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. These measures include, as appropriate:

- Use of reputable infrastructure providers that apply industry-standard security practices.
- Encryption of data in transit.
- Access controls to ensure that only authorised personnel and systems can access personal data.
- Limitation of the personal data collected and processed to what is necessary for the purposes described in this Privacy Policy.

No method of transmission over the Internet or method of electronic storage is completely secure, and we cannot guarantee absolute security. However, we seek to maintain an appropriate level of security in accordance with applicable laws and industry standards.

12. Links to Other Services

The App or our website may contain links to third-party services, including our Substack page for newsletters.

If you subscribe to our newsletter directly on Substack or otherwise interact with Substack, your personal data will be processed by Substack in accordance with its own terms and privacy policy. This Privacy Policy does not govern Substack's processing of your personal data.

We recommend that you review the privacy policies of any third-party services you use.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time, for example to reflect changes in the App, our data processing activities, or applicable legal requirements.

When we make changes, we will:

- Update the "Last updated" date at the top of this Privacy Policy; and
- Where required by law or where changes are material, provide additional notice within the App or by other appropriate means (for example, email).

Your continued use of the App after the effective date of any updated Privacy Policy constitutes your acceptance of the updated terms. If you do not agree with the updated Privacy Policy, you should stop using the App and may request deletion of your account.

14. Contact Us

If you have any questions, requests, or concerns regarding this Privacy Policy or our processing of personal data, you may contact us at:

Atnias LLC

Email: support@atnias.com