AIRA
Artificial Intelligence Real-time Artist

PRIVACY POLICY

Last Updated: May 20, 2026 ("Effective Date")

Introduction

VenFira Private Limited ("VenFira", "we", "us" or "our"), a company incorporated under the laws of India with its registered office in Pune, Maharashtra, India, is committed to protecting Your privacy and the security of Your personal data.

This Privacy Policy explains how we collect, use, store, share and protect Your personal data when You use the AIRA application (the "Program"), our website at https://thepocketdj.com (the "Website"), and any related services (collectively, the "Services").

AIRA collects and processes sensitive data, including Biometric Data (such as heart rate and activity data). Please read this Privacy Policy carefully, particularly Sections 4 and 5, to understand how we handle such data.

By using the Services, You acknowledge that You have read and understood this Privacy Policy. If You do not agree with this Privacy Policy, please do not use the Services.

This Privacy Policy should be read in conjunction with our End User Licence Agreement ("EULA") and Terms and Conditions, available at https://thepocketdj.com/legal.

1. Data Controller

The data controller responsible for Your personal data is:

VenFira Private Limited
Bengaluru, Karnataka, India
Email: ashok@venfira.com
Website: https://thepocketdj.com

For EU/EEA and UK users, if we appoint a representative under Article 27 of the GDPR, their details will be published on our Website.

2. Data We Collect

We collect and process the following categories of personal data:

2.1 Account and Registration Data

Data Type	Examples	Purpose
Identity Data	Name, email address	Account creation, licence activation, communication
Licence Data	Licence key, machine ID, subscription tier, activation status	Licence verification, feature gating, subscription management
Payment Data	Payment method details, transaction history, billing address	Subscription payment processing (handled by third-party payment processors)
Device Data	Machine ID (hashed hardware UUID), device model, operating system version	Licence verification, device management, compatibility

2.2 Usage and Analytics Data

Data Type	Examples	Purpose
App Usage Data	Features used, session duration, mixing mode, transition strategies selected, playback events	Product improvement, analytics, feature development
Library Metadata	Number of tracks, genres, BPM distribution (aggregated, not individual track data)	Product improvement, tier limit enforcement
Error and Crash Data	Crash reports, error logs, diagnostic data	Bug fixing, stability improvement
Performance Data	CPU/memory usage, audio latency metrics	Performance optimization

2.3 Audio Analysis Data

Data Type	Examples	Purpose

Track Metadata	BPM, musical key, energy level, genre classification, vocal detection results, cue points, waveform data	Core Program functionality — audio analysis, intelligent mixing, transition optimization
AI Model Data	Anonymized and aggregated analysis patterns	AI model training and improvement

Platform-Specific Storage:

(a) AIRA Mac (Desktop): Audio Analysis Data is generated and stored locally on Your device only. Your music files are never transmitted to our servers. Analysis is performed entirely on-device using local CoreML models.

(b) AIRA iOS (Mobile — Regular Users): When You upload a track for analysis, Your audio file is temporarily uploaded to AWS S3 (`temp-analysis/` path) for server-side analysis. Once analysis is complete, the audio file is automatically deleted from S3. Your audio files are not retained on our servers — playback occurs from Your local device. Only the resulting Audio Analysis Data (track metadata such as BPM, key, genre, energy, cue points) is stored on our servers in a PostgreSQL database linked to Your user account. This enables features such as metadata sync and BPM-based recommendations.

(b-ii) AIRA iOS (Producers): If You upload tracks as a Producer, Your audio files and cover art are stored persistently on AWS S3 for streaming to other users. These files remain on S3 until You delete them from Your library or request account deletion.

(c) BPM Cache (Shared): When BPM data is discovered for a track (via analysis, Apple Music API, or third-party sources), the track title, artist, and BPM value (without any user-identifying information) may be contributed to a shared BPM cache to improve BPM lookup accuracy for all users. This data is anonymized and cannot be traced back to any individual user.

2.4 Biometric Data (Sensitive Data)

Data Type	Examples	Purpose
Heart Rate Data	Current heart rate, heart rate variability, resting heart rate	Biometric DJ mode — adapting music tempo and energy to Your physiological state
Activity Data	Activity type (walking, running, resting, cycling, driving), step count, workout session data	Context-aware music adaptation

Motion Data	Accelerometer and gyroscope data	Activity detection, motion-responsive music features

Biometric Data is only collected if You explicitly enable Biometric DJ features and grant the necessary device permissions. See Section 4 for detailed Biometric Data provisions.

2.5 Communication Data

Data Type	Examples	Purpose
Support Communications	Emails, chat messages, feedback	Customer support, product improvement
Survey Responses	Feedback, ratings, feature requests	Product development

2.6 Automatically Collected Data

Data Type	Examples	Purpose
Log Data	IP address, browser type, access times, pages viewed (Website only)	Security, analytics
Cookies and Similar Technologies	Session cookies, analytics cookies (Website only)	Website functionality, analytics (see Section 10)

3. How We Use Your Data

3.1 Legal Bases for Processing (GDPR)

For users in the European Economic Area (EEA), United Kingdom (UK) and other jurisdictions that require a legal basis for processing, we rely on the following:

Legal Basis	Data Categories	Purpose
Contract Performance (Art. 6(1)(b) GDPR)	Account Data, Licence Data, Device Data, Audio Analysis Data	Providing the Program's core functionality, managing Your account, processing subscriptions
Legitimate Interests (Art. 6(1)(f) GDPR)	Usage Data, Performance Data, Error Data, aggregated Analytics	Product improvement, security, fraud prevention, customer support
Explicit Consent (Art. 6(1)(a) / Art. 9(2)(a) GDPR)	Biometric Data, marketing communications, cookies (where required)	Biometric DJ features, personalized communications, website analytics
Legal Obligation (Art. 6(1)(c) GDPR)	Account Data, Payment Data	Tax compliance, legal reporting, responding to lawful requests

3.2 Purposes of Processing

We use Your personal data for the following purposes:

(a) Providing and Operating the Program
- Licence activation and verification
- Subscription management and feature gating
- Audio analysis and intelligent mixing functionality
- Biometric DJ features (with Your explicit consent)
- Discovery and music recommendation features
- Cloud sync and backup (if applicable)

(b) Improving the Program
- Analyzing aggregated and anonymized usage patterns to improve AI algorithms
- Identifying and fixing bugs and performance issues
- Developing new features and functionality
- Training and improving machine learning models using anonymized data

(c) Communication
- Sending transactional communications (licence confirmations, subscription receipts, update notifications)
- Responding to support requests
- Sending product updates and release notes
- Marketing communications (only with Your consent, where required)

(d) Security and Fraud Prevention
- Detecting and preventing unauthorized access, licence abuse or fraud
- Monitoring system integrity and security
- Enforcing our EULA and Terms and Conditions

(e) Legal Compliance
- Complying with applicable laws, regulations and legal processes
- Responding to lawful requests from public authorities

4. Biometric Data — Special Provisions

Given the sensitive nature of Biometric Data, this section provides detailed information about how we handle such data.

4.1 What Biometric Data We Collect

If You enable Biometric DJ features, the Program may access the following through Your device's APIs (e.g., Apple HealthKit, CoreMotion, WatchConnectivity):

- Heart rate — current BPM, resting heart rate, heart rate variability
- Activity type — walking, running, cycling, resting, driving, workout sessions
- Motion data — accelerometer and gyroscope readings for activity detection
- Workout data — workout type, duration, intensity (if applicable)

4.2 How Biometric Data Is Processed

(a) On-Device Processing. Your Biometric Data is processed exclusively on Your device. The Program reads biometric sensors and health data APIs locally to adapt music playback in real time. Raw Biometric Data is not transmitted to VenFira's servers unless You explicitly opt in to a cloud-based feature that requires it (if any such feature is offered).

(b) No Persistent Storage. The Program processes Biometric Data in real-time, in-memory. It does not save, log or persistently store Your raw Biometric Data to disk or to any database.

(c) No Third-Party Sharing. We do not share, sell, rent, lease, trade or disclose Your Biometric Data to any third party for any purpose, including advertising, marketing, analytics or profiling.

(d) No Profiling or Automated Decision-Making. We do not use Your Biometric Data for profiling, automated decision-making, insurance, employment, credit or any purpose other than real-time music adaptation within the Program.

4.3 Legal Basis for Biometric Data Processing

- GDPR (EU/EEA/UK): We process Biometric Data solely on the basis of Your explicit consent under Article 9(2)(a) of the GDPR. You may withdraw consent at any time (see Section 7).

- BIPA (Illinois, USA): We comply with the Illinois Biometric Information Privacy Act. We obtain informed, written consent before collecting Biometric Data, do not sell or profit from it, and store and protect it using reasonable security measures.
- CCPA/CPRA (California, USA): Biometric Data is treated as "sensitive personal information" under the CPRA. You have the right to limit the use and disclosure of sensitive personal information.
- DPDP Act (India): We process Biometric Data in accordance with India's Digital Personal Data Protection Act, 2023, and obtain Your consent before processing.
- LGPD (Brazil): We comply with Brazil's Lei Geral de Proteção de Dados and process Biometric Data only with Your explicit consent.
- Privacy Act (Australia): Biometric Data is treated as "sensitive information" under the Australian Privacy Act 1988, and we collect it only with Your consent.

4.4 How to Control Biometric Data Collection

You can control Biometric Data collection at any time by:

(a) Disabling Biometric DJ features within the Program's Settings;

(b) Revoking Health/Motion permissions in Your device's system settings (e.g., Settings → Privacy & Security → Health → AIRA on iOS/macOS);

(c) Disconnecting Your wearable device from the Program;

(d) Contacting us at ashok@venfira.com to request deletion of any Biometric Data we may hold.

4.5 Biometric Data Retention

Since Biometric Data is processed in real-time on Your device and not persistently stored, there is no Biometric Data to retain or delete on our servers. If any Biometric Data is transmitted to our servers (e.g., through an opt-in cloud feature), it will be retained only for as long as necessary to provide the feature and will be deleted upon Your request or withdrawal of consent.

5. Data Sharing and Disclosure

5.1 Service Providers

We may share Your personal data with the following categories of service providers who process data on our behalf:

Service Provider	Purpose	Data Shared

Payment Processors (e.g., LemonSqueezy, Stripe, Apple)	Subscription payment processing	Payment Data, Account Data
Cloud Infrastructure (e.g., AWS, Railway)	Backend services hosting	Account Data, Licence Data, Usage Data
Analytics Providers	Aggregated usage analytics	Anonymized Usage Data
Email Service Providers	Transactional and marketing emails	Email address, name
Error Tracking	Crash reporting and diagnostics	Error Data, Device Data

All service providers are bound by data processing agreements and are required to process Your data only for the purposes specified by us.

5.2 We Do NOT Share

- Your music files or audio content (Mac) — never transmitted to our servers; all analysis is performed locally
- Your music files (iOS — Regular Users) — temporarily uploaded to our servers solely for analysis, then automatically deleted from S3 after analysis completes; playback occurs from Your local device
- Your music files (iOS — Producers) — stored on AWS S3 for streaming to other users; You may delete them at any time from Your library
- Your Biometric Data — never shared with any third party
- Your Audio Analysis Data (Mac) — stored locally on Your device; only anonymized aggregates used for AI improvement
- Your Audio Analysis Data (iOS) — stored on our servers linked to Your account; deleted upon Your request or account deletion

- Your personal data for advertising purposes — we do not sell Your data to advertisers

5.3 Legal Disclosure

We may disclose Your personal data if required to do so by law, regulation, legal process or governmental request, or if we believe in good faith that such disclosure is necessary to:

(a) Comply with a legal obligation;

(b) Protect and defend our rights or property;

(c) Prevent or investigate possible wrongdoing in connection with the Services;

(d) Protect the personal safety of users or the public; or

(e) Protect against legal liability.

5.4 Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy or sale of all or a portion of our assets, Your personal data may be transferred as part of such transaction. We will notify You of any such change and any choices You may have regarding Your personal data.

6. International Data Transfers

6.1 Transfer Mechanisms

VenFira is based in India. Your personal data may be transferred to and processed in countries other than Your country of residence, including India and the United States (where our cloud infrastructure may be located).

For transfers of personal data from the EEA, UK or Switzerland to countries not deemed to provide an adequate level of data protection, we rely on the following safeguards:

(a) Standard Contractual Clauses (SCCs) approved by the European Commission;

(b) UK International Data Transfer Agreements (IDTAs) or UK Addendum to the EU SCCs, as applicable;

(c) Adequacy decisions by the European Commission or UK Secretary of State, where available; or

(d) Your explicit consent to the transfer, where other safeguards are not available.

6.2 India — DPDP Act

For users in India, we process Your personal data in accordance with the Digital Personal Data Protection Act, 2023 (DPDP Act). We will transfer personal data outside India only to countries or territories notified by the Central Government as permissible destinations, or in accordance with conditions prescribed under the DPDP Act.

6.3 Your Right to Object

You may contact us at ashok@venfira.com to obtain more information about the safeguards we have put in place for international data transfers.

7. Your Rights

Depending on Your jurisdiction, You may have the following rights regarding Your personal data:

7.1 Rights Under GDPR (EU/EEA) and UK GDPR

Right	Description
Right of Access (Art. 15)	You have the right to obtain confirmation of whether we process Your personal data and to access a copy of such data.
Right to Rectification (Art. 16)	You have the right to request correction of inaccurate or incomplete personal data.
Right to Erasure ("Right to be Forgotten") (Art. 17)	You have the right to request deletion of Your personal data, subject to certain exceptions.
Right to Restriction of Processing (Art. 18)	You have the right to request restriction of processing of Your personal data in certain circumstances.
Right to Data Portability (Art. 20)	You have the right to receive Your personal data in a structured, commonly used, machine-readable format.
Right to Object (Art. 21)	You have the right to object to processing based on legitimate interests or for direct marketing purposes.

Right to Withdraw Consent (Art. 7(3))	Where processing is based on consent (including Biometric Data), You may withdraw consent at any time without affecting the lawfulness of processing performed prior to withdrawal.
Right Not to be Subject to Automated Decision-Making (Art. 22)	You have the right not to be subject to decisions based solely on automated processing, including profiling, that produces legal or similarly significant effects.
Right to Lodge a Complaint	You have the right to lodge a complaint with a supervisory authority in Your member state.

7.2 Rights Under CCPA/CPRA (California, USA)

Right	**Description**
Right to Know	You have the right to know what personal information we collect, use, disclose and sell.
Right to Delete	You have the right to request deletion of Your personal information.
Right to Opt-Out of Sale	We do not sell Your personal information. If this changes, You will have the right to opt out.
Right to Limit Use of Sensitive Personal Information	You have the right to limit the use and disclosure of sensitive personal information (including Biometric Data).
Right to Non-Discrimination	You have the right not to receive discriminatory treatment for exercising Your privacy rights.
Right to Correct	You have the right to request correction of inaccurate personal information.

California "Shine the Light" Law: California residents may request information about our disclosure of personal information to third parties for their direct marketing purposes. We do not disclose personal information to third parties for their direct marketing purposes.

Do Not Track: We do not currently respond to "Do Not Track" browser signals.

7.3 Rights Under DPDP Act (India)

Right	Description
Right to Access	You have the right to obtain a summary of Your personal data and the processing activities carried out on it.
Right to Correction and Erasure	You have the right to request correction of inaccurate or misleading data, completion of incomplete data, updating of data and erasure of data no longer necessary for the purpose for which it was collected.
Right to Grievance Redressal	You have the right to submit a grievance to our designated Grievance Officer (see Section 13).
Right to Nominate	You have the right to nominate another individual to exercise Your rights in the event of Your death or incapacity.

7.4 Rights Under LGPD (Brazil)

Brazilian users have rights to: confirmation of processing, access, correction, anonymization/ blocking/deletion of unnecessary data, data portability, information about sharing, information about consent, and revocation of consent.

7.5 Rights Under the Privacy Act (Australia)

Australian users have rights under the Australian Privacy Principles (APPs), including the right to access, correct, and complain about handling of personal information.

7.6 How to Exercise Your Rights

To exercise any of the above rights, please contact us at:

- Email: ashok@venfira.com

- Subject Line: "Privacy Rights Request — [Your Right]"

We will respond to Your request within:
- 30 days for GDPR/UK GDPR requests (extendable by 60 days for complex requests)
- 45 days for CCPA/CPRA requests (extendable by 45 days)
- 30 days for DPDP Act requests
- 30 days for LGPD requests

We may request verification of Your identity before processing Your request.

8. Data Retention

8.1 Retention Periods

Data Category	Retention Period
Account Data	Duration of Your account + 30 days after deletion request
Licence Data	Duration of Your licence + 1 year for audit purposes
Payment Data	As required by applicable tax and financial regulations (typically 7 years)
Usage Data	2 years from collection (anonymized and aggregated after this period)
Audio Analysis Data (Mac)	Stored locally on Your device; deleted when You uninstall the Program or manually delete
Audio Analysis Data (iOS)	Metadata stored on our servers (Railway/ PostgreSQL) linked to Your account; audio files temporarily uploaded to S3 for analysis then automatically deleted; metadata deleted when You delete individual tracks or upon account deletion request
Producer Audio Files (iOS)	Stored on AWS S3 for streaming; deleted when You delete individual tracks or upon account deletion request
BPM Cache Data	Anonymized track BPM data stored indefinitely in shared database; not linked to any user account
Biometric Data	Not persistently stored; processed in real-time and discarded
Error/Crash Data	1 year from collection

Communication Data	3 years from last communication
Cookie Data	See Cookie Policy (Section 10)

8.2 Deletion

Upon termination of Your account or upon Your request, we will delete or anonymize Your personal data within the timeframes specified above, unless retention is required by applicable law or for the establishment, exercise or defence of legal claims.

8.3 Local Data

8.3 Local Data (Mac)

On AIRA Mac, Audio Analysis Data, preferences and cached data are stored locally on Your device and are under Your control. You may delete this data by uninstalling the Program or clearing the Program's data in Your device settings.

8.4 Server-Stored Data (iOS)

On AIRA iOS, Audio Analysis Data (metadata only) is stored on our servers (PostgreSQL on Railway) linked to Your user account. When You upload a track for analysis, the audio file is temporarily stored on AWS S3 and is automatically deleted after analysis completes. Your audio files are not retained on our servers — playback occurs from Your local device. For Producer accounts, uploaded audio files and cover art are stored persistently on AWS S3 for streaming to other users. You may delete individual tracks and their associated analysis data at any time from within the app. Upon account deletion, all associated Audio Analysis Data, and any Producer audio files, will be permanently deleted from our servers within 30 days. BPM Cache Data (anonymized, not linked to Your account) is retained indefinitely to benefit all users.

9. Data Security

9.1 Security Measures

We implement appropriate technical and organizational measures to protect Your personal data against unauthorized access, alteration, disclosure, destruction or accidental loss, including:

(a) Encryption in Transit: All data transmitted between Your device and our servers is encrypted using TLS 1.2 or higher.

(b) Encryption at Rest: Personal data stored on our servers is encrypted at rest using industry-standard encryption algorithms.

(c) Access Controls: Access to personal data is restricted to authorized personnel on a need-to-know basis, with role-based access controls and multi-factor authentication.

(d) Secure Infrastructure: Our backend services are hosted on enterprise-grade cloud platforms with ISO 27001 and SOC 2 certifications.

(e) Licence Security: Machine IDs are generated using a one-way cryptographic hash (SHA-256) of hardware identifiers, ensuring that raw hardware identifiers are not stored or transmitted.

(f) On-Device Processing: Sensitive data (including Biometric Data and audio content) is processed locally on Your device wherever possible, minimizing server-side exposure.

(g) Regular Security Reviews: We conduct regular security assessments and vulnerability testing.

9.2 Data Breach Notification

In the event of a personal data breach that is likely to result in a risk to Your rights and freedoms, we will:

(a) Notify the relevant supervisory authority within 72 hours of becoming aware of the breach (as required by GDPR Art. 33);

(b) Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms (GDPR Art. 34);

(c) Comply with any additional breach notification requirements under applicable law (e.g., CCPA, DPDP Act, LGPD, Australian Privacy Act).

9.3 Your Responsibilities

You are responsible for maintaining the security of Your account credentials, licence key and device access. We recommend using strong, unique passwords and enabling device-level security features (e.g., FileVault, Face ID, Touch ID).

10. Cookies and Similar Technologies

10.1 Website Cookies

Our Website (https://thepocketdj.com) may use the following types of cookies:

Cookie Type	Purpose	Duration
Strictly Necessary	Essential for Website functionality (e.g., session management, security)	Session
Analytics	Understanding how visitors use the Website (e.g., page views, traffic sources)	Up to 2 years
Functional	Remembering Your preferences (e.g., language, region)	Up to 1 year
Marketing	Delivering relevant advertisements (only with Your consent)	Up to 1 year

10.2 Consent

For users in the EU/EEA, UK and other jurisdictions requiring cookie consent, we will obtain Your consent before placing non-essential cookies on Your device. You may manage Your cookie preferences through the cookie banner displayed on our Website.

10.3 How to Manage Cookies

You can control cookies through Your browser settings. Please note that disabling certain cookies may affect Website functionality.

10.4 The Program

The AIRA application (Mac/iOS) does not use cookies. Local data storage within the Program uses standard application data directories and UserDefaults, not browser cookies.

11. Children's Privacy

11.1 Age Requirements

The Services are not intended for children under the age of:

- 16 years in the EU/EEA (or the applicable age in Your member state)
- 13 years in the United States
- 18 years in India
- 13 years in other jurisdictions (unless local law specifies otherwise)

11.2 No Knowingly Collection

We do not knowingly collect personal data from children under the applicable age. If we become aware that we have collected personal data from a child without appropriate parental consent, we will take steps to delete such data promptly.

11.3 Parental Rights

If You are a parent or guardian and believe that Your child has provided personal data to us, please contact us at ashok@venfira.com so that we can take appropriate action.

12. Third-Party Links and Services

12.1 Third-Party Links

The Services may contain links to third-party websites or services. We are not responsible for the privacy practices or content of such third parties. We encourage You to review the privacy policies of any third-party services You access.

12.2 Third-Party Integrations

The Program may integrate with third-party services, including:

- Apple HealthKit / Health app — for Biometric Data (heart rate, activity)
- Apple Watch / WatchConnectivity — for wearable device data
- CoreMotion — for motion and activity data
- Music streaming services — for catalog access (if integrated)
- Payment processors — for subscription payments
- Auto-update services (Sparkle) — for software update checks

Each integration is subject to the third party's own privacy policy and terms of service. We only access data from these integrations as necessary to provide Program functionality and with Your explicit permission.

12.3 Apple HealthKit Compliance

If the Program accesses Apple HealthKit data:

(a) We will not use HealthKit data for advertising or marketing purposes;

(b) We will not sell HealthKit data to third parties;

(c) We will not use HealthKit data for purposes unrelated to providing the Program's health-related features;

(d) HealthKit data will not be disclosed to third parties without Your explicit consent, except as required by law; and

(e) We comply with Apple's HealthKit guidelines and review requirements.

13. Contact Information and Grievance Officer

13.1 General Privacy Inquiries

For any questions, concerns or requests regarding this Privacy Policy or our data practices, please contact:

VenFira Private Limited — Privacy Team
Email: ashok@venfira.com
Website: https://thepocketdj.com/privacy

13.2 Data Protection Officer

If we appoint a Data Protection Officer (DPO), their contact details will be published on our Website.

13.3 Grievance Officer (India — DPDP Act / IT Act)

In accordance with the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000, we have designated the following Grievance Officer:

Grievance Officer
Email: ashok@venfira.com
Response Time: Within 30 days of receipt of complaint

13.4 Supervisory Authorities

If You are in the EU/EEA or UK and believe that our processing of Your personal data infringes applicable data protection law, You have the right to lodge a complaint with Your local supervisory authority. A list of EEA supervisory authorities is available at: https://edpb.europa.eu/about-edpb/about-edpb/members_en

For UK residents, You may contact the Information Commissioner's Office (ICO) at: https://ico.org.uk

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. We will notify You of any material changes by:

(a) Posting the updated Privacy Policy on our Website with a new "Last Updated" date;

(b) Sending You an email notification (for material changes affecting Your rights);

(c) Displaying an in-app notification when You next use the Program.

We encourage You to review this Privacy Policy periodically. Your continued use of the Services after any changes constitutes Your acceptance of the updated Privacy Policy.

15. California Privacy Disclosures (CCPA/CPRA)

15.1 Categories of Personal Information Collected

In the preceding 12 months, we have collected the following categories of personal information:

Category	Collected	Source

Identifiers (name, email, account ID)	Yes	Directly from You
Payment information	Yes	Directly from You (via payment processor)
Internet activity (usage data, logs)	Yes	Automatically collected
Geolocation (approximate, IP-based)	Yes	Automatically collected
Biometric information	Yes (with consent)	From Your device sensors/ wearables
Professional/employment information	No	N/A
Education information	No	N/A
Audio/visual information	No (we do not access Your music content on our servers)	N/A
Inferences	Yes (genre preferences, usage patterns)	Derived from usage data
Sensitive personal information	Yes (Biometric Data, with consent)	From Your device sensors/ wearables

15.2 Sale and Sharing of Personal Information

We do not sell Your personal information as defined by the CCPA/CPRA. We do not share Your personal information for cross-context behavioral advertising.

15.3 Retention

See Section 8 for data retention periods.

16. Jurisdiction-Specific Provisions

16.1 European Economic Area (EEA) and United Kingdom

- Legal bases for processing are set out in Section 3.1.
- International transfer safeguards are described in Section 6.
- Your rights under GDPR/UK GDPR are described in Section 7.1.
- Data breach notification procedures are described in Section 9.2.

16.2 United States

- California residents: see Section 15 for CCPA/CPRA disclosures.
- Illinois residents: see Section 4.3 for BIPA compliance.

- We comply with applicable state privacy laws, including the Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA) and other state privacy laws as they take effect.

16.3 India

- We comply with the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Information Technology Act, 2000.
- Grievance Officer details are provided in Section 13.3.
- We obtain consent before processing personal data as required by the DPDP Act.
- We transfer personal data outside India only in accordance with the DPDP Act.

16.4 Brazil

- We comply with the Lei Geral de Proteção de Dados (LGPD).
- Brazilian users' rights are described in Section 7.4.
- We process personal data based on consent, legitimate interest, or contract performance as applicable.

16.5 Australia

- We comply with the Privacy Act 1988 and the Australian Privacy Principles (APPs).
- Australian users' rights are described in Section 7.5.
- Biometric Data is treated as "sensitive information" under the APPs.

16.6 Canada

- We comply with the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws.
- We obtain meaningful consent for the collection, use and disclosure of personal information.

16.7 Japan

- We comply with the Act on the Protection of Personal Information (APPI).
- We handle personal information in accordance with the APPI's requirements for consent, purpose limitation and cross-border transfers.

16.8 South Korea

- We comply with the Personal Information Protection Act (PIPA).
- We process personal information based on consent and provide required disclosures.