SONOVIA APP, INC.
PRIVACY POLICY

Version 1.0 | Last Updated: 8 September 2026

Sonovia App, Inc. ("Sonovia," "we," "us," or "our") is a Delaware corporation that operates a travel, cultural-content, and location-based audio-tour platform. This Privacy Policy applies to the Sonovia mobile application, our website at https://sonovia.app, creator and content-provider tools, customer support, and other online or offline services that link to or expressly reference this Policy (collectively, the "Services").

For purposes of the EU General Data Protection Regulation ("GDPR"), the UK GDPR, Turkey's Law No. 6698 on the Protection of Personal Data ("KVKK"), and similar laws, Sonovia is generally the controller or data controller of the personal information described in this Policy, unless a separate notice states otherwise.

This Policy does not govern the independent privacy practices of Apple, Google, payment providers, mapping providers, creators, venues, museums, tourism businesses, or other third parties. Their own policies apply when they independently determine how and why they process personal information.

Information We Collect

The information we collect depends on how you interact with the Services, which features you use, your device settings, and the permissions you grant.

Account and Contact Information

We may collect your name, username, email address, authentication identifiers from your sign-in provider (Apple, Google or email), preferred language, country or region, profile details, account settings, and other information you provide when creating or managing an account.

Location Information

With your permission, we may collect precise or approximate location information from your device to identify nearby tours and places, trigger location-based audio or content, display maps and routes, provide location-aware recommendations, improve features, prevent misuse, and support safety or security functions. We may also infer a general location from an IP address or device settings. You can change location permissions through your device settings, but some features may not function without them.

Device, Usage, and Technical Information

We may automatically collect IP address, device identifiers, device type, operating system, app version, language, time zone, network information, crash reports, diagnostics, performance data, security events, access times, pages or screens viewed, links selected, session information, feature interactions, tour progress, and listening history.

Device Permissions and Media

Depending on the features you choose, the Services may request access to notifications, camera, microphone, photo library, Bluetooth, motion sensors, local storage, or other device functions. If you upload or record material, we may process photos, videos, audio or voice recordings, captions, transcripts, metadata, and related files. Sonovia does not use voice, photographs, or videos to create biometric identifiers or uniquely identify a person unless we first provide a specific notice and obtain any consent required by law.

Purchases, Subscriptions, and Commercial Information

We may collect records of tours, subscriptions, digital content, or other products you view, purchase, redeem, or access; transaction date and amount; currency; subscription and entitlement status; refund or cancellation information; app-store receipt or transaction identifier; and related customer-service records. Purchases through Apple App Store or Google Play are processed under the applicable platform's payment and privacy terms. Sonovia generally does not receive full payment-card numbers from those platforms.

User Content and Communications

We may collect reviews, ratings, comments, messages, reports, support requests, survey responses, dispute notices, infringement or takedown submissions, and any photos, audio, video, tour materials, or other content you submit. Content you intentionally publish or share through public or community features may be visible to other users, creators, venues, or the public.

Creator and Content-Provider Information

If you are a creator, guide, author, translator, narrator, photographer, videographer, performer, interviewee, museum, venue, tourism business, agency, or other contributor, we may collect professional and business contact information, biography and profile information, portfolio and content files, ownership and licensing records, releases and consents, identity or authority verification, tax information, payout information, revenue-share records, contracts, invoices, communications, performance information, moderation history, and complaint or infringement records.

Information From Third Parties

We may receive information from app stores, authentication providers, payment and payout providers, creators, venues, business partners, security providers, sign-in services (Apple and Google), public sources, and other users. For example, an app store may confirm a purchase or subscription, a creator may provide information needed to document rights or attribution, and another user may submit a report involving your content or account.

Cookies and Similar Technologies

Our website and web-based features use only local storage that is strictly necessary to keep you signed in and to remember your language preference. We do not use cookies, pixels, software development kits, or similar technologies for advertising, analytics, or cross-site tracking.

Sensitive Information

Depending on your use of the Services, we may process information considered sensitive under some laws, such as precise geolocation, government identification or tax information for creator verification, financial account or payout information, private communications, or content that you choose to provide and that reveals sensitive characteristics. We process sensitive information only for disclosed, reasonably necessary purposes, with appropriate safeguards, and with consent where required.

How We Collect Information

- **Directly from you**, including when you create an account, make a purchase, upload content, contact support, submit a rights request, or participate as a creator.
- **Automatically from your device and use of the Services**, including through permissions, logs, and local storage.
- **From platforms and service providers**, such as Apple, Google, payment or payout providers, authentication services, hosting providers, mapping services, and security providers.
- **From creators, business partners, other users, and public sources**, when they provide information relevant to content rights, attribution, reports, transactions, or the operation of the Services.

How We Use Information

- Provide and operate the Services, including accounts, tours, maps, location-based features, content access, subscriptions, purchases, downloads, and creator tools.
- Authenticate users, maintain sessions, remember preferences, synchronize entitlements, and provide customer support.
- Process and document purchases, subscriptions, refunds, creator payouts, revenue sharing, taxes, accounting, and related records.
- Personalize and recommend tours, locations, languages, creators, or content based on settings, general or precise location where enabled, and prior activity.
- Receive, host, review, approve, reject, publish, license, attribute, moderate, investigate, restrict, or remove User Content and Creator Content.
- Verify content ownership, licenses, permissions, releases, creator identity or authority, and compliance with contracts and platform rules.
- Communicate about accounts, purchases, updates, security, support, and policies.
- Analyze performance, diagnose errors, develop new features, conduct research, and improve the safety, accessibility, quality, and usability of the Services.
- Detect, prevent, investigate, and respond to fraud, abuse, infringement, security incidents, unlawful activity, violations of our terms, and risks to users or the public.
- Comply with law, legal process, tax and accounting duties, sanctions and export requirements, consumer-protection obligations, and enforceable governmental requests.

- Establish, exercise, or defend legal claims; enforce agreements; protect Sonovia, users, creators, venues, and others; and support corporate transactions.
- Create aggregated or de-identified information that is not reasonably capable of identifying an individual, and use it for lawful business purposes.

Legal Bases for Processing

Where the GDPR, UK GDPR, KVKK, or another law requires a legal basis, Sonovia relies on one or more of the following bases, as applicable:

- **Contract.** Processing is necessary to enter into or perform a contract with you, such as providing an account, purchased tour, subscription, creator relationship, payout, or customer support.
- **Legitimate interests.** Processing is necessary for Sonovia's or another party's legitimate interests, such as operating and improving the Services, securing systems, preventing fraud, enforcing agreements, personalizing content, and supporting ordinary business operations, provided those interests are not overridden by your rights and interests.
- **Legal obligation.** Processing is necessary to comply with tax, accounting, consumer, privacy, sanctions, court-order, recordkeeping, or other legal duties.
- **Consent.** We rely on consent where required, including for certain device permissions, precise location features, or sensitive information. You may withdraw consent at any time, without affecting processing that occurred before withdrawal.
- **Vital interests and legal claims.** In limited circumstances, processing may be necessary to protect a person's vital interests or to establish, exercise, or defend legal claims.

For processing subject to KVKK, Sonovia relies on the applicable conditions in Articles 5 and 6, including explicit consent where required; necessity for forming or performing a contract; compliance with legal obligations; establishment, exercise, or protection of a right; information made public by the data subject within the intended scope; and legitimate interests that do not harm fundamental rights and freedoms.

How We Disclose Information

We may disclose personal information to the following categories of recipients for the purposes described in this Policy:

- Service providers and processors that support cloud hosting, storage, content delivery, account authentication, crash reporting, customer support, communications, mapping, location services, security, fraud prevention, moderation, accessibility, and professional services.
- Apple, Google, payment, subscription, and payout providers to complete transactions, verify entitlements, process refunds, make creator payments, prevent fraud, and maintain required financial records.

- Creators, venues, museums, tourism businesses, agencies, and other marketplace participants when needed to provide requested content, document rights, facilitate a transaction, investigate a complaint, or carry out a relationship you direct.
- Other users or the public when you intentionally publish content, a profile, a review, attribution information, or other material through a public feature.
- Professional advisers, auditors, insurers, banks, accountants, and legal counsel when reasonably necessary for business, compliance, risk-management, or legal purposes.
- Government authorities, courts, regulators, law enforcement, and other parties when required by law or reasonably necessary to protect rights, safety, security, and the integrity of the Services.
- A buyer, investor, lender, successor, or other transaction participant in connection with a financing, merger, acquisition, reorganization, sale of assets, bankruptcy, or similar corporate event, subject to appropriate safeguards.
- Other parties with your direction or consent.

Some content you provide is processed by third-party artificial-intelligence and audio services. Voice and audio recordings you upload are sent to these providers for transcription, audio isolation and speech synthesis, and recordings, photographs and tour text are sent for automated quality and moderation review. Support messages you send us are processed by a third-party artificial-intelligence provider to help answer your request. These providers are identified by name in our Data Collection and Processing Policy.

Sale, Sharing, and Targeted Advertising

Sonovia does not sell personal information for monetary consideration. Unless Sonovia provides a separate notice and legally required opt-out mechanism, Sonovia does not use or disclose personal information for cross-context behavioral advertising in a manner treated as a "sale" or "sharing" under California law. We do not knowingly sell or share the personal information of individuals under 16 years of age. If these practices change, we will update this Policy and provide required choices before the change applies.

Public Content and the Creator Ecosystem

The Services may allow users and creators to submit or publish reviews, profiles, tours, audio, photographs, videos, maps, captions, transcripts, credits, and other materials. Information you choose to make public may be copied, saved, indexed, reshared, or used by others outside Sonovia's control. Do not include private, confidential, or sensitive information in public content unless you intend it to be public and have the right to disclose it.

Sonovia may review content and associated information to verify rights, moderate the Services, investigate reports, enforce agreements, prevent harm, and comply with law. When content is rejected, restricted, or removed, Sonovia may retain limited records of the submission, decision, notices, ownership evidence, complaints, and transactions as reasonably necessary for compliance, dispute resolution, fraud prevention, and legal claims.

Location and Device Controls

Mobile operating systems generally require you to grant permission before an app accesses precise location, camera, microphone, photographs, notifications, Bluetooth, motion, or similar device functions. You can review or revoke permissions in your device settings. Revoking a permission does not delete information previously collected, but you may request deletion where applicable. Certain features, including nearby-tour discovery, route functions, recorded content, or notifications, may not work after a permission is disabled.

The Services are not emergency, navigation, or safety services. Location information may be delayed or inaccurate. Privacy choices do not replace the need to follow official directions, posted signs, current conditions, and applicable safety rules.

Do Not Track Signals

Browser-based Do Not Track signals are not governed by a single uniform standard, so our response may vary.

Data Retention

We retain personal information only for as long as reasonably necessary for the purposes described in this Policy, including to provide the Services, maintain security and business records, comply with legal duties, resolve disputes, enforce agreements, and establish or defend claims. Retention depends on the nature of the information and the context in which it was collected.

- Account and profile information is generally retained while the account is active and for a reasonable period afterward to complete deletion, prevent fraud, resolve disputes, and satisfy legal obligations.
- Purchase, subscription, payout, tax, accounting, and creator-contract records are retained for the periods required by applicable financial, tax, corporate, and limitation laws.
- Precise location is retained only as long as reasonably necessary to provide the requested feature, maintain security, troubleshoot, or satisfy a user-selected function.
- User Content and Creator Content may be retained while published or licensed and afterward as needed for backups, transaction history, takedown records, rights verification, dispute resolution, and legal compliance.
- Support communications, moderation records, security logs, consent records, and rights-request records are retained for a period reasonably related to their operational, evidentiary, security, and legal purposes.

When retention is no longer justified, we take reasonable steps to delete, anonymize, or securely isolate the information. Residual copies may remain temporarily in backups or where deletion is technically impracticable, subject to access restrictions and deletion cycles.

Security

We use administrative, technical, and physical safeguards designed to protect personal information, taking into account the nature of the information and the risks of processing. Measures may include access controls, authentication, encryption in transit where appropriate, logging, backups, vendor controls, secure development practices, incident response, and personnel confidentiality requirements. No system or transmission method is completely secure, and we cannot guarantee absolute security. You are responsible for protecting your credentials and notifying us promptly of suspected unauthorized account access.

International Data Transfers

Sonovia is based in the United States and may use personnel and service providers in the United States, Turkey, the European Economic Area, the United Kingdom, and other countries. As a result, personal information may be processed in a country whose laws differ from those where you live.

For transfers subject to the GDPR or UK GDPR, Sonovia uses an available lawful transfer mechanism where required, such as an adequacy decision, the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or UK Addendum, or an applicable derogation, together with supplementary safeguards where appropriate. For transfers subject to KVKK, Sonovia uses an available mechanism under Article 9, such as an adequacy decision, an approved standard contract, binding corporate rules where applicable, another approved undertaking, or a limited statutory exception. You may contact us for additional information about applicable safeguards.

Your Choices

- **Account information.** You may review or update certain account details through the Services or by contacting us.
- **Device permissions.** You may manage location, camera, microphone, photographs, notifications, Bluetooth, motion, and similar permissions through device settings.
- **Marketing communications.** We do not currently send marketing email. If that changes, we will provide an unsubscribe link and, where required, ask for consent first. We will continue to send transactional, legal, and security communications.
- **Public content.** You may delete or edit certain content through available controls. Copies, transaction records, legal records, or content reshared by others may remain.
- **Account deletion.** You may request account deletion through available in-app controls or by contacting us. Deleting your account does not remove everything immediately. Tours you have published are removed from public listings but remain playable for 365 days by people who purchased them before your account was deleted, so that they receive what they paid for. Financial ledger entries, sales and payout records, and tax documents are kept as accounting records and are not deleted with your account, because we are required to retain them. If you are a creator with a positive balance when you delete your

account, we will still pay that balance out to you. Other information may be retained as explained in Data Retention.

Privacy Rights and How to Exercise Them

Depending on where you live and subject to legal exceptions, you may have the right to request access to personal information, obtain a copy, correct inaccurate information, delete information, restrict or object to processing, withdraw consent, receive portable data, opt out of certain sales, sharing, targeted advertising, or profiling, limit certain uses of sensitive information, and appeal a denied request.

To submit a privacy request, contact us at support@sonovia.app. Please state that your request concerns privacy and identify the right you wish to exercise. We may request information reasonably necessary to verify your identity, account, authority, and jurisdiction. We will use verification information only for verification and compliance purposes.

You may use an authorized agent where law permits. We may require proof of the agent's authority and may ask you to verify your identity directly. We will respond within the period required by applicable law. If we deny a request, we will explain the basis where required and provide appeal instructions when applicable. We will not unlawfully discriminate against you for exercising a privacy right.

California Privacy Notice

This section supplements the rest of the Policy for California residents. It applies if and to the extent Sonovia is a "business" subject to the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the "CCPA"). Where Sonovia is not legally required to honor a CCPA request, it may choose to do so voluntarily.

For the 12 months preceding the Last Updated date, depending on which Services and features were available and used, Sonovia collected or may have collected the categories described below. Sonovia expects to collect the same categories during the next 12 months when relevant features are used.

Categories of Personal Information

Identifiers and customer-record information. Name, username, postal or email address, IP address, account identifier, authentication information, and, for creators or payees, identity, tax, financial, or business records.

Commercial information. Purchase, subscription, entitlement, refund, payout, transaction, and content-access history.

Internet or electronic-network activity. Device, browser, app, session, interaction, diagnostics, crash, security, and usage information.

Geolocation information. Approximate location and, when permission is enabled, precise device location.

Audio, electronic, visual, and similar information. Voice recordings, audio, photographs, video, uploaded files, transcripts, captions, and support or moderation materials.

Professional, commercial, and creator information. Professional profiles, portfolios, business contacts, contracts, authority and ownership records, licensing documentation, attribution, invoices, and creator-performance information.

Protected characteristics. Information such as age range, language, disability or accessibility information, nationality, or other characteristics only when you voluntarily provide it or when reasonably necessary and lawful.

Inferences. Preferences or recommendations derived from location, language, purchases, listening history, interactions, or content interests.

Sensitive personal information. Precise geolocation, private communications, and, for creators or payees where needed, government identification, tax information, or financial account and payout information.

Biometric information. Sonovia does not collect biometric information for the purpose of uniquely identifying an individual unless a separate feature-specific notice and legally required consent are provided.

Sources, Purposes, and Recipients

We obtain these categories from you, your device, app stores and service providers, creators and business partners, other users, connected services you choose, and public sources. We use them for the business and commercial purposes described in the How We Use Information section. We disclose them to the recipient categories described in the How We Disclose Information section. The exact categories disclosed depend on the service performed and the information reasonably necessary for that service.

Sale, Sharing, and Sensitive Personal Information

Sonovia does not sell personal information for money. Unless a separate notice states otherwise, Sonovia does not sell or share personal information for cross-context behavioral advertising. Sonovia uses and discloses sensitive personal information only for purposes reasonably necessary to provide requested services, secure accounts and systems, process creator or payee relationships, comply with law, and perform other purposes permitted without a right to limit under the CCPA. If these practices change, Sonovia will provide any required notice and opt-out or limitation mechanism.

During the preceding 12 months, Sonovia disclosed or may have disclosed the categories listed above to the service providers, contractors, platforms, marketplace participants, professional advisers, authorities, and transaction parties described in How We Disclose Information, solely for the business purposes stated in this Policy and as permitted by law. Sonovia did not sell those categories for money and, unless a separate notice states otherwise, did not share them for cross-context behavioral advertising.

California Retention Criteria

For each California category, Sonovia applies the retention principles in Data Retention and the following category-specific criteria:

- Identifiers, customer-record information, protected characteristics, and inferences are retained while reasonably needed for the account, requested personalization, support, security, fraud prevention, disputes, and applicable legal duties.
- Commercial, professional, creator, payout, tax, and transaction information is retained for the applicable contract, transaction, accounting, tax, corporate, audit, and legal-claims periods.
- Internet, device, diagnostics, and security information is retained for operational, analytics, troubleshooting, cybersecurity, fraud-prevention, and legal-evidence cycles proportionate to the associated risk.
- Precise geolocation is retained only as long as reasonably necessary for the requested location feature, security, troubleshooting, or a user-selected function.
- Audio, visual, User Content, and Creator Content is retained while submitted, published, licensed, or transactionally relevant and afterward as needed for rights verification, backups, takedowns, disputes, and legal compliance.
- Sensitive personal information is retained no longer than reasonably necessary for the service, verification, security, payout, compliance, or legal purpose for which it was collected.

California Rights

- Right to know and access the categories and specific pieces of personal information collected, sources, purposes, and recipient categories.
- Right to delete personal information, subject to exceptions.
- Right to correct inaccurate personal information.
- Right to opt out of sale or sharing, if applicable.
- Right to limit certain uses or disclosures of sensitive personal information, if applicable.
- Right to receive information about financial incentives, if any, and to avoid discriminatory treatment for exercising CCPA rights.

Submit a request using the methods in Privacy Rights and How to Exercise Them. If Sonovia engages in sale or sharing in the future, it will provide a conspicuous "Do Not Sell or Share My Personal Information" mechanism and honor valid opt-out preference signals, including Global Privacy Control, as required. Sonovia does not currently offer a financial incentive or price or service difference in exchange for personal information.

European Economic Area and United Kingdom

If the GDPR or UK GDPR applies, the sections above describe the identity of the controller, categories and sources of personal data, purposes and legal bases, recipients, international transfers, retention criteria, and available rights.

- You may request access, rectification, erasure, restriction, and data portability, subject to applicable conditions and exceptions.
- You may withdraw consent at any time for future processing based on consent.
- You may lodge a complaint with the supervisory authority in the country where you live, work, or believe a violation occurred. In the United Kingdom, the supervisory authority is the Information Commissioner's Office.

Right to object. You have the right to object at any time to processing based on legitimate interests, including related profiling. You also have the right to object at any time to processing for direct marketing, including related profiling. We will stop the affected processing unless a legally permitted exception applies.

Sonovia may use automated systems to rank or recommend tours and content, detect fraud or security risks, and support moderation. Sonovia does not currently use solely automated processing to make decisions that produce legal or similarly significant effects about ordinary users. If that changes, Sonovia will provide any notice and rights required by law.

Where Article 27 of the GDPR or an equivalent UK requirement requires Sonovia to appoint a local representative, the representative's current contact details will be made available in the Services and at https://docs.sonovia.app/sonovia-privacy-policy-en.pdf.

Turkey - KVKK Notice

For processing subject to KVKK, Sonovia App, Inc. is the data controller unless a separate notice identifies another controller. Sonovia's identity and contact details appear in Contact Us below.

Purposes and recipients. Sonovia processes personal data for the specific purposes described in How We Use Information and may transfer data to the recipient groups described in How We Disclose Information, limited to what is necessary and lawful.

Collection methods and legal grounds. Personal data may be collected electronically through the mobile application, website, account and transaction screens, device permissions, emails, forms, creator tools, contracts, app stores, service providers, business partners, other users, and public sources. Legal grounds include the applicable processing conditions under KVKK Articles 5 and 6, as described in Legal Bases for Processing.

International transfers. Personal data may be transferred outside Turkey only through a mechanism permitted by KVKK Article 9 and applicable secondary legislation, including an adequacy decision, approved standard contract or undertaking, binding corporate rules where applicable, or a limited statutory exception.

Your KVKK Article 11 rights may include learning whether personal data is processed; requesting information about processing; learning the purpose of processing and whether data is used accordingly; learning recipients in Turkey or abroad; requesting correction of incomplete or inaccurate data and notification to recipients; requesting deletion or destruction when legal

conditions are met and notification to recipients; objecting to an adverse result arising from analysis exclusively by automated systems; and requesting compensation for damage caused by unlawful processing. Submit requests using the contact methods below. Sonovia may request information necessary to verify identity and authority.

Age Requirement

The Services are intended for adults. A person under 18 may not create an account or use the Services, and Sonovia does not knowingly collect personal information from anyone under 18. Sonovia also does not knowingly collect personal information online from a child under 13 without verifiable parental consent where required by the U.S. Children's Online Privacy Protection Act. If you believe a person under 18 has provided personal information to Sonovia, contact us so we can investigate, delete the information, and close the account.

Because the Services are not offered to anyone under 18, Sonovia does not rely on parental or guardian authorization for any processing. If Sonovia becomes aware that an account belongs to a person under 18, it will close the account and delete the associated personal information, subject to any legal retention duty.

Third-Party Services and Links

The Services may link to or interoperate with app stores, mapping tools, payment services, venues, creator websites, social platforms, or other third-party services. Sonovia is not responsible for a third party's independent privacy practices. Review the third party's privacy notice before providing information or enabling an integration.

Changes to This Policy

We may update this Policy to reflect changes in the Services, technology, law, vendors, or business practices. We will post the revised Policy with a new Last Updated date and provide additional notice or obtain consent when required. Material changes apply prospectively unless law permits otherwise.

Contact Us

Questions, complaints, and privacy requests may be directed to:

Sonovia App, Inc.
2010 Crow Canyon Place, Suite 100 PMB# 17480244, San Ramon, California 94583

Email: support@sonovia.app

Please include "Privacy Request" in the subject line and describe the request. Do not send passwords, full payment-card numbers, or unnecessary sensitive information by email.