# SHMONG LEGAL POLICIES & AGREEMENTS

*Last Updated: April 25, 2025*
*Effective Date: April 25, 2025*

# SHMONG LEGAL POLICIES & AGREEMENTS

*Last Updated: April 25, 2025 Effective Date: April 25, 2025*

---

# SECTION 1: TERMS OF SERVICE

## SUMMARY

This Terms of Service governs your use of SHMONG services. It explains your rights and responsibilities, payment terms, arbitration procedures, and other legal matters. By using our services, you agree to these terms. These Terms include important provisions like arbitration requirements, limitations of liability, and your responsibilities when uploading content containing biometric data of other individuals.

## 1. ELIGIBILITY AND ACCOUNT CREATION

1.1. **Age Restriction.** You must be at least 18 years old to create an account and use our Services.

1.2. **Account Creation.** To access certain features, you may need an account. You agree to provide accurate, current, and complete information during registration and keep it updated.

1.3. **Electronic Communications Consent.** By creating an account, you consent to receive electronic communications from us. These may include service notifications, security notices, and legal updates. You may opt out of marketing emails but not service-critical communications.

1.4. **SMS and Mobile Communications.** If you provide a mobile number, you consent to receive SMS/mobile messages. Standard rates may apply. Reply “STOP” to opt out.

## 2. USER CONTENT AND RESPONSIBILITY

2.1. **Responsibility for Content and Consent.** You are solely responsible for all Content you upload and for obtaining all necessary permissions, including: - Explicit, informed, written consent from all individuals whose biometric identifiers appear in

your Content - Consent from parents/guardians for any minors depicted - Permissions for any property, trademarks, or copyrighted material shown

2.2. **Primary Accountability.** As the uploader, you accept primary and sole legal responsibility for obtaining proper biometric consent from individuals in your Content. You agree to defend and indemnify SHMONG against claims arising from your failure to obtain proper consent.

2.3. **Consent Record Requirements.** As an uploader, you agree to: - Maintain verifiable written consent records for all individuals in your Content - Preserve these records for at least five (5) years from upload - Provide records to SHMONG within seven (7) business days upon request - Update consents if new data uses arise not covered initially

2.4. **Copyright Ownership.** You warrant that you own the copyright to the Content you upload or have obtained express permission from the owner.

## 3. LICENSE GRANT AND DATA USAGE

3.1. **License to Use Content.** By providing Content, you grant SHMONG a non-exclusive, worldwide, royalty-free, sublicensable license to use, reproduce, modify, adapt, publish, translate, distribute, and display such Content solely in connection with providing, maintaining, securing, and improving the Services.

3.2. **Anonymized and Aggregated Data.** You agree SHMONG may create and use aggregated and anonymized datasets derived from Content and usage data for any purpose, including research, analytics, or commercial use, provided it complies with applicable laws.

3.3. **Commercial Data Usage.** By accepting this Agreement, you expressly authorize SHMONG to commercially use your biometric data as detailed in Section 1.3 of the Biometrics Policy (Section 3 of this document). This includes using anonymized biometric data for commercial purposes across all jurisdictions, and other

commercial uses as permitted by the laws in your state of residence. Please refer to the Biometrics Policy for complete details on how we collect, use, store, protect, and share biometric data.

## 4. SUBSCRIPTION AND PAYMENT TERMS

4.1. **Subscription Services.** Some features may require a paid subscription. By subscribing, you agree to pay all associated fees.

4.2. **Billing and Payment.** For paid subscriptions: - You agree to provide accurate billing information - Subscription fees will be billed in advance on either a monthly or annual basis - All payments are non-refundable except as expressly stated or required by law - We reserve the right to change prices with notice, effective at your next billing cycle

4.3. **Free Trials.** We may offer free trials. Unless you cancel before the trial ends, you authorize us to charge your payment method. No notice will be sent that your free trial has ended.

4.4. **Subscription Renewal and Cancellation.** Your subscription will automatically renew unless you cancel before the renewal date.

## 5. USER CONDUCT AND RESTRICTIONS

5.1. **Compliance with Laws.** Use the Services in compliance with all applicable laws and regulations.

5.2. **Prohibited Content.** Do not upload, share, or create Content that: - Violates third-party rights - Contains biometric data without proper consent - Depicts minors without parental consent - Is defamatory, obscene, pornographic, offensive, or threatening - Promotes illegal activities - Contains malware or harmful code

5.3. **Username and Content Policies.** When creating usernames, profiles, or sharing content: - Usernames must not impersonate others or infringe on trademarks - Usernames and profile content must not contain offensive, obscene, or hateful language - Display names and profile images must comply with our Content guidelines - You may not use misleading or deceptive identifiers - SHMONG

reserves the right to remove or reclaim usernames, particularly those related to brands or notable individuals - Profile information must be accurate and not misleading - SHMONG may reject, reclaim, or remove any username for any reason, including trademark claims - Dormant accounts with desirable usernames may be reclaimed after 12 months of inactivity

## 6. ARBITRATION AND DISPUTE RESOLUTION

6.1. **Binding Arbitration.** Any dispute arising from these Terms shall be resolved exclusively through binding arbitration, except that either party may seek equitable relief in any court of competent jurisdiction.

> **In Plain Language:** If we have a disagreement about these Terms, we'll resolve it through arbitration (a private dispute resolution process) instead of going to court. The only exception is if either of us needs immediate court help to stop ongoing harm.

6.2. **Arbitration Process.** Arbitration shall be conducted in Delaware, pursuant to the rules of the American Arbitration Association (AAA) or JAMS. The arbitration award will be final and binding.

6.3. **Opt-Out Option.** You have the right to opt out of arbitration by notifying SHMONG in writing at Legal@shmong.com, or sending written notice to our Delaware address within 60 days of accepting these Terms. If you opt-out, all disputes will be resolved in accordance with the laws of Delaware and subject to the appropriate courts, rather than through arbitration. The written notice must clearly state your intent to opt-out of arbitration.

> **In Plain Language:** You can choose not to participate in arbitration if you tell us in writing within 60 days of agreeing to these terms. If you opt out, any disputes would go through regular courts instead.

6.4. **Class Action Waiver.** You agree that disputes will be resolved on an individual basis only, not as part of a class action. You waive any right to participate in class actions.

> **In Plain Language:** By using our service, you agree to handle any disputes with us one-on-one, not as part of a group lawsuit.

## 7. CHOICE OF LAW AND VENUE

7.1. **Choice of Law.** These Terms shall be governed by Delaware law, without regard to conflicts of law principles.

7.2. **Venue.** Disputes not subject to arbitration shall be resolved exclusively in Delaware courts. You agree to submit to the personal jurisdiction of such courts.

## 8. INDEMNIFICATION

8.1. **User Indemnification.** You agree to defend, indemnify, and hold harmless SHMONG from any claims, liabilities, damages, losses, costs, or fees arising from your violation of these Terms, your Content (including lack of consent), or violation of third-party rights.

## 9. LIMITATION OF LIABILITY

9.1. **"AS IS" Basis.** THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE," WITHOUT WARRANTIES OF ANY KIND.

9.2. **Limitation of Liability.** TO THE FULLEST EXTENT PERMITTED BY LAW, SHMONG SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING FROM YOUR USE OF THE SERVICES.

9.3. **Cap on Liability.** SHMONG's total liability for all claims arising under these Terms shall be limited to the amount you paid to SHMONG in the last 12 months prior to the claim. This limitation applies regardless of the basis of any liability claim and regardless of the form of action.

> **In Plain Language:** If something goes wrong, we'll only be responsible for refunding what you've paid us in the past year. This limit applies no matter what type of legal claim might be involved.

## 10. MODIFICATION OF TERMS

10.1. **Changes to Terms.** SHMONG reserves the right to modify these Terms of Service at any time. For material changes to these Terms: - We will provide at least 30 days' notice before the changes take effect - Notice will be provided through email (for registered users) and prominent notice on our website - We will highlight significant changes and provide a summary of modifications - For non-material changes, updates may take effect immediately upon posting

10.2. **Acceptance of Modified Terms.** After the notice period, your continued use of the Services constitutes acceptance of the modified Terms. If you do not agree to the updated terms, you must stop using the Services and terminate your account.

10.3. **Prior Versions.** We will maintain an archive of previous versions of these Terms for your reference.

## 11. GENERAL PROVISIONS

11.1. **Severability.** If a provision is unenforceable, it will be limited or eliminated minimally; the rest remains in effect.

11.2. **Assignment.** You cannot assign Terms without SHMONG's consent; SHMONG may assign freely.

11.3. **Entire Agreement.** These Terms constitute the entire agreement, superseding prior agreements.

11.4. **No Third Party Beneficiaries.** These Terms are not intended to confer rights to any third parties.

11.5. **Force Majeure.** Neither party is liable for delays due to causes beyond reasonable control.

11.6. **Contact.** Questions about Terms: Legal@shmong.com

## 12. COPYRIGHT AND INTELLECTUAL PROPERTY

12.1. **DMCA Policy.** SHMONG respects intellectual property rights and expects users to do the same. We will respond to notices of alleged copyright infringement that comply with applicable law.

12.2. **Reporting Copyright Infringement.** If you believe your copyrighted work has been used in a way that constitutes copyright infringement, please submit a notification containing: - Physical or electronic signature of the copyright owner or authorized agent - Identification of the copyrighted work claimed to be infringed - Identification of the material that is claimed to be infringing - Your contact information (address, telephone number, email) - Statement that you have a good faith belief that use of the material is not authorized - Statement that the information is accurate and, under penalty of perjury, you are authorized to act on behalf of the copyright owner

12.3. **DMCA Agent.** Submit copyright infringement notifications to: - DMCA Agent, SHMONG - Legal@shmong.com - [Physical Address]

12.4. **Counter Notification.** If you believe your content was removed due to a mistake or misidentification, you may submit a counter-notification containing: - Your physical or electronic signature - Identification of the material removed and its former location - Statement under penalty of perjury that you have a good faith belief

the material was removed as a result of mistake or misidentification - Your consent to the jurisdiction of the federal court in Delaware - Your contact information

12.5. **Repeat Infringer Policy.** SHMONG maintains a policy of terminating accounts of repeat infringers in appropriate circumstances. We reserve the right to terminate accounts that receive multiple copyright infringement notices.

## 13. EXPORT CONTROL COMPLIANCE

13.1. **Export Restrictions.** The Services, including any biometric technologies and software, may be subject to U.S. export laws, including the Export Administration Regulations and sanctions programs administered by the Office of Foreign Assets Control.

13.2. **User Compliance Obligations.** You agree not to: - Export or re-export our Services to any prohibited country, entity, or person - Access or use the Services in any U.S. embargoed countries (currently Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions) - Use the Services for activities prohibited by export laws, including nuclear, chemical, or biological weapons development - Transfer, export, or re-export the Services without required governmental authorizations

> **In Plain Language:** You cannot use our service in countries under U.S. embargo (like Cuba or North Korea) or share it with people on U.S. government restricted lists. You also can't use our technology for weapons development or other prohibited activities.

13.3. **Representation.** By using the Services, you represent and warrant that you are not located in a country subject to U.S. embargo or designated as a "terrorist supporting" country, and you are not listed on any U.S. government list of prohibited or restricted parties.

13.4. **Compliance with Laws.** You are responsible for complying with all domestic and international export laws and regulations that apply to your use of the Services.

## DEFINITIONS

- **"Content"**: Any images, videos, text, audio, or other materials uploaded, shared, or created using our Services.
- **"User"**: Any individual who accesses or uses our Services, whether registered or unregistered.
- **"Consent"**: Informed, written consent obtained through these Terms or the Biometric Data Consent Agreement.
- **"Services"**: Our website, mobile application, and related services, including face matching system.
- **"Arbitration"**: A process for resolving disputes outside of court where a neutral third party makes a binding decision.
- **"Force Majeure"**: Unforeseeable circumstances that prevent the fulfillment of a contract, such as natural disasters or war.

## 6. ACCOUNT TERMINATION

6.1. **Account Termination by User.** You may terminate your account at any time by: - Selecting "Delete Account" in account settings - Sending a deletion request to Legal@shmong.com - Upon confirmation, your account will be deactivated immediately and scheduled for permanent deletion within 30 days - Content you've publicly shared may remain visible unless specifically deleted prior to account termination

6.2. **Account Termination by SHMONG.** SHMONG may suspend or terminate your account: - For violations of these Terms - For extended periods of inactivity (12+ months) - If required by law or court order - If we suspect fraudulent activity or misrepresentation - If you fail to pay fees after reasonable attempts to collect - For any other reason at our discretion with reasonable notice

6.3. **Effect of Termination.** Upon termination: - Your access to the Services will cease immediately - You will lose access to any content stored within your account - Subscription charges will cease at the end of the billing period - Your biometric data will be deleted according to our Biometrics Policy - You remain liable for any outstanding obligations incurred before termination - Provisions of these Terms that by their nature should survive will remain in effect

---

# SECTION 2: PRIVACY POLICY

## SUMMARY

This Privacy Policy explains what information we collect, how we use it, and your rights regarding your data. We collect personal information, usage data, and in some cases biometric data. We implement security measures to protect your information and provide you with control over your data through various rights and options. Special provisions apply for residents of certain states and countries.

## 1. INFORMATION WE COLLECT

1.1. **Personal Information.** We collect information you provide when you: - Create an account (name, email, phone number) - Use our services - Contact customer support - Participate in surveys or promotions

1.2. **Automatically Collected Information.** We automatically collect: - Device information (IP address, browser type, operating system) - Usage information (pages visited, features used, time spent) - Location information (approximate location based on IP address)

1.3. **Biometric Data.** If you use our face matching features, we may collect biometric data as described in the Biometrics Policy.

## 2. HOW WE USE YOUR INFORMATION

2.1. **Provide and Improve Services.** We use your information to: - Deliver the services you request - Personalize your experience - Develop new features and improvements - Analyze usage patterns and trends

2.2. **Communications.** We may use your information to: - Send service announcements and updates - Respond to your inquiries - Provide customer support - Send marketing communications (with consent)

2.3. **Security and Fraud Prevention.** We use information to: - Protect the security of our services - Prevent fraudulent activity - Enforce our Terms of Service

## 3. DATA SHARING AND DISCLOSURE

3.1. **No Sale of Personal Information.** We do not sell, lease, trade, or otherwise profit from your personal information.

3.2. **Limited Disclosure.** We may share information with: - Service providers helping us deliver our services - Legal authorities when required by law or legal process - In connection with a merger, acquisition, or sale of assets

3.3. **Third-Party Service Providers.** We work with the following third parties who may receive or process your data: - Stripe: For payment processing and subscription management - Amazon Web Services: For cloud storage and computing infrastructure - Google: For analytics, authentication, and cloud services - Dropbox: For file storage and synchronization - Mixpanel: For user behavior analytics and engagement tracking

These third parties access and process your information only to perform specific tasks on our behalf and are obligated not to disclose or use your information for any other purpose. Each is bound by data processing agreements that require appropriate security and confidentiality measures.

3.4. **Third-Party Services.** Our services may integrate with third-party services. Information shared with these services is governed by their respective privacy policies.

## 4. DATA RETENTION AND DELETION

4.1. **Retention Period.** We retain your personal information for as long as necessary to provide our services and fulfill the purposes described in this policy.

4.2. **Data Deletion.** You may request deletion of your personal information. We will delete your information within 45 days of a verified request, unless retention is required by law.

## 5. USER DATA RIGHTS

5.1. **Access.** You have the right to access your personal data and information about its processing.

5.2. **Correction.** You can request correction of inaccurate personal information.

5.3. **Deletion.** You can request deletion of your personal information.

5.4. **Portability.** You may request a copy of your data in a structured, machine-readable format.

5.5. **Withdraw Consent.** You may withdraw consent for personal data processing at any time.

5.6. **Exercise Rights.** Contact Legal@shmong.com to exercise these rights. We will respond within the timeframe required by applicable law.

## 6. COOKIES AND TRACKING TECHNOLOGIES

6.1. **Cookies.** We use cookies and similar technologies to enhance your experience, gather information about users, and manage our services. These include: - **Essential Cookies**: Required for the service to function (cannot be disabled) - **Functional Cookies**: Enhance functionality and personalization - **Analytics Cookies**: Help

us understand how users interact with our service - **Advertising Cookies**: Used to deliver relevant ads and track campaign effectiveness

6.2. **Managing Cookies.** You can manage cookie preferences through: - Our cookie banner and preference center - Your browser settings - Opting out of specific third-party cookies via their opt-out mechanisms

6.3. **Do Not Track.** We respond to Do Not Track signals by disabling all non-essential tracking when detected.

6.4. **Similar Technologies.** In addition to cookies, we also use: - Web beacons - Pixel tags - Local storage - Device fingerprinting - Mobile analytics software

## 7. INTERNATIONAL USERS

7.1. **Data Transfers.** Your information may be transferred to and processed in countries other than your country of residence.

7.2. **Legal Basis for Processing.** For users in the European Economic Area, United Kingdom, or similar jurisdictions, we process your data based on: - Your consent - Performance of a contract - Legitimate interests - Compliance with legal obligations

7.3. **Region-Specific Rights.** Users in certain regions have additional rights as detailed in the Biometrics Policy.

## 8. CALIFORNIA PRIVACY RIGHTS

8.1. **California Consumer Privacy Act (CCPA/CPRA) Rights.** California residents have the following rights: - Right to know what personal information is collected, used, shared, or sold - Right to delete personal information collected from you - Right to opt-out of the sale of your personal information - Right to correct inaccurate personal information - Right to limit use and disclosure of sensitive personal information - Right to non-discrimination for exercising your rights

8.2. **California "Shine the Light" Law.** California residents may request information regarding disclosure of personal information to third parties for direct marketing purposes.

8.3. **Exercise Your California Rights.** Submit requests by: - Visiting our privacy portal at privacy.shmong.com - Emailing Legal@shmong.com - Calling 1-800-XXX-XXXX

8.4. **Authorized Agents.** You may designate an authorized agent to make requests on your behalf.

8.5. **Verification Process.** We will verify your identity before fulfilling requests, which may require additional information.

8.6. **Response Timeline.** We will respond to verifiable requests within 45 days, with possible 45-day extension if reasonably necessary.

## 9. CHILDREN'S PRIVACY

9.1. **Age Restrictions.** Our services are not directed to individuals under 18. We do not knowingly collect personal information from children.

9.2. **Parental Rights.** Parents or guardians may contact us to review, modify, or delete their child's information if we have inadvertently collected it.

## 10. DETAILED GDPR COMPLIANCE

10.1. **Legal Basis for Processing.** For EEA, UK, and Swiss residents, we process personal data on these legal bases: - Consent (Article 6(1)(a) GDPR): When you explicitly agree to processing - Contractual Necessity (Article 6(1)(b) GDPR): To perform our contract with you - Legal Obligation (Article 6(1)(c) GDPR): To comply with legal requirements - Legitimate Interests (Article 6(1)(f) GDPR): When we have legitimate business interests

10.2. **GDPR Data Subject Rights.** You have the following rights: - Access (Article 15): Obtain confirmation and access to your personal data - Rectification (Article 16): Correct inaccurate

personal data - Erasure (Article 17): Request deletion of personal data - Restriction (Article 18): Limit how we use your data while a request is processed - Portability (Article 20): Receive your data in a structured, machine-readable format - Objection (Article 21): Object to processing based on legitimate interests - Automated Decision-Making (Article 22): Not be subject to automated decision-making with legal effects

10.3. **Data Transfers.** For transfers outside the EEA, UK, or Switzerland: - We use European Commission approved Standard Contractual Clauses - We implement supplementary measures as recommended by the EDPB - We conduct transfer impact assessments for high-risk transfers

10.4. **Data Protection Officer.** You may contact our Data Protection Officer at dpo@shmong.com.

10.5. **Supervisory Authority.** You have the right to lodge a complaint with your local supervisory authority.

## 11. DATA SECURITY

11.1. **Security Measures.** We implement technical, administrative, and physical safeguards to protect your information.

11.2. **Data Breach Notification.** In the event of a data breach, we will notify affected users as required by applicable law.

## 12. LAW ENFORCEMENT DATA REQUESTS

12.1. **Government Requests.** SHMONG may disclose personal information, including biometric data, in response to: - Valid subpoenas, court orders, warrants, or similar legal processes - National security letters, requests from government agencies, or as otherwise required by law - Requests to protect the safety of any person, to address fraud or illegal activity, or to protect SHMONG's rights or property

12.2. **Request Evaluation Process.** We carefully review all legal requests to ensure they satisfy applicable legal requirements and our policies. We may: - Request clarification or additional information - Narrow overly broad requests - Object to requests we determine are improper - Notify users of requests when not prohibited by law or court order

12.3. **User Notification.** Unless prohibited by law or court order (e.g., sealed court orders, confidentiality obligations): - We will attempt to notify users of legal demands for their data - We will provide users with copies of the legal request when possible - We may delay notification where immediate notification could risk harm, safety, or fraud

12.4. **Transparency Reporting.** SHMONG publishes periodic transparency reports summarizing: - Number and types of government requests received - Our response rates - Number of accounts affected - Jurisdictional breakdown of requests

12.5. **International Requests.** For requests from non-U.S. government agencies, we require: - Due process under applicable laws - Mutual Legal Assistance Treaties or similar international agreements - Compliance with U.S. law and our policies

## DEFINITIONS

- **"Personal Information"**: Information that identifies or can be used to identify an individual.
- **"Biometric Data"**: Information based on biological characteristics, such as facial geometry, that can be used to identify an individual.
- **"Data Controller"**: The entity that determines the purposes and means of processing personal data.
- **"Data Processor"**: The entity that processes personal data on behalf of the data controller.
- **"IP Address"**: A unique string of numbers assigned to each device connected to a computer network.

- **“Cookies”**: Small text files stored on your device that help websites remember your preferences and track usage.

---

# SECTION 3: BIOMETRICS POLICY

## SUMMARY

This Biometrics Policy governs how we collect, use, store, and protect biometric data. We collect biometric identifiers like facial geometry only with your explicit consent for specific purposes, such as face matching services. We implement strong security measures to protect this sensitive data and provide you with rights to access, delete, or withdraw consent for your biometric information. Special provisions apply based on your state or country of residence.

## 1. BIOMETRIC DATA COLLECTION AND CONSENT

1.1. **Collection Authorization.** SHMONG maintains a publicly available written policy detailing retention schedules and destruction guidelines for Biometric Data. By accepting this Agreement, you consent to the collection, storage, use, and processing of your Biometric Data (e.g., facial geometry, templates, vectors derived from your Content).

1.2. **Specific Biometric Identifiers Collected.** SHMONG explicitly collects and processes the following biometric identifiers: - Facial geometry and landmarks - Facial measurement vectors and templates - Facial recognition data points - Mathematical representations of facial features - Other facial biometric data necessary for our facial recognition technology

1.3. **Commercial Data Usage.** By accepting this Agreement, you expressly authorize SHMONG to: - Sell, trade, share, and commercially use your biometric data - Generate revenue from insights derived from biometric data - License biometric data to third parties for commercial purposes - Create and monetize products based on biometric data - Transfer or assign rights to biometric data as part of business operations

By accepting this Agreement, you explicitly consent to these commercial activities. We may engage in these commercial activities while maintaining reasonable security measures for your data as outlined in this Agreement.

1.4. **Rights Waiver.** By accepting this Agreement, you acknowledge and agree to waive the following rights regarding your biometric data: - The right to revoke consent for historical data usage that has already been incorporated into our systems - The right to restrict certain forms of processing necessary for core service functionality - The right to object to legitimate commercial usage as permitted by applicable law and described in this Policy - The right to disable certain security features that rely on biometric authentication - Any rights beyond those explicitly granted in this Agreement or required by applicable law

You retain all other rights not explicitly waived, including those detailed in Section 3 of this Biometrics Policy, and your right to opt-out as described in Section 1.5 remains unaffected by this waiver.

1.5. **Opt-Out Procedure.** You may opt out of biometric data collection, processing, and commercial usage at any time by: - Emailing a clear request to Legal@shmong.com with the subject line “Biometric Data Opt-Out” - Including your account information and specific opt-out request details - Verifying your identity through our standard verification process

Upon receipt of a verified opt-out request, SHMONG will: - Cease collecting new biometric data within 10 business days - Delete existing biometric data within 45 days (subject to legal retention requirements) - Confirm completion of your opt-out request - Note that opting out may limit or disable certain features that rely on biometric data

1.6. **Uploader Responsibility.** If you upload content containing other individuals, you are solely and exclusively responsible for obtaining their written consent, notifying them of this policy, and documenting their acceptance as specified in the Terms of Service. SHMONG’s role is limited to requiring uploaders to certify they have obtained proper consent before uploading biometric data.

1.7. **Certification of Consent by Uploaders.** Before uploading any Content containing biometric data of other individuals, you must certify that: - You have obtained express, informed written consent from each identifiable individual - You have informed these individuals that their biometric data will be processed by SHMONG - You maintain verifiable records of these consents - You take full legal responsibility for the consent collection process - You will indemnify SHMONG against any claims arising from inadequate consent

1.8. **Mandatory Certification Checkbox.** SHMONG implements a mandatory certification process requiring uploaders to affirmatively check a box before each upload containing biometric data, specifically certifying they have obtained all necessary consents. This checkbox is non-optional, and uploads cannot proceed without this certification. SHMONG maintains records of these certifications, including timestamps and user information. However, SHMONG does not independently verify the actual consent documents and relies entirely on uploader certifications.

1.9. **SHMONG's Limited Role in Consent Process.** SHMONG's role regarding consent is limited to: - Requiring uploaders to certify they have obtained proper consent - Providing uploaders with information about consent requirements - Establishing a mechanism for certification during the upload process - Maintaining records of uploader certifications SHMONG does not verify the actual consent documents obtained by uploaders and relies entirely on uploader certifications regarding consent.

> **In Plain Language:** If you upload photos of other people to our service: - You must check a box confirming you have their permission - You are responsible for actually getting their written permission - We keep a record of your certification but don't check the actual permission forms - We trust that when you check the box, you've truly gotten proper permission - You are legally responsible if you upload someone's face without proper permission

1.10. **Consent Verification and Audit Program.** To ensure the integrity of our consent certification system: - SHMONG conducts periodic random audits of uploader consent records to verify compliance - Selected uploaders must provide verifiable evidence of proper consent within 10 business days - Uploaders agree to participate in these audits as a condition of using our Services - Audits will assess both the existence and validity of consent records - SHMONG will maintain detailed records of all audit processes and findings - Audit frequency will be determined based on risk assessment and usage volume

1.11. **Consequences of Audit Failure.** Failure to comply with audit requirements or discovery of consent violations may result in: - Immediate account suspension pending investigation - Permanent account termination for serious or repeated violations - Removal of all Content uploaded without proper consent documentation - Prohibition from creating new accounts on the platform - Potential reporting to relevant regulatory authorities - Legal action for indemnification as provided in the Terms of Service - Additional remedial measures as required to ensure compliance

> **In Plain Language:** - We will randomly check if uploaders actually have the permission forms they claimed to have - If selected for audit, you must show us the permission documents within 10 business days - If you can't prove you had permission or you've falsely claimed to have permission, we may suspend or terminate your account, remove your content, ban you from our platform, report you to authorities, and/or take legal action against you

## 2. STORAGE AND PROTECTION

2.1. **Duration of Storage.** We retain Biometric Data until the earliest of: - For Texas residents, not later than the first anniversary of the date the purpose for collecting the identifier expires - For Illinois residents, when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the

individual's last interaction, whichever occurs first - For residents of other states, three (3) years after last interaction - Your deletion request fulfillment - Failure to provide re-consent

> **In Plain Language:** We'll keep biometric data until: - For Texas residents: for no more than 1 year after we no longer need it - For Illinois residents: until we no longer need it or for 3 years after last activity, whichever happens first - For other states: for up to 3 years after last activity - Earlier if you ask us to delete it or don't renew your consent when asked

2.2. **Security Standards.** We store, transmit, and protect Biometric Data using a reasonable standard of care within our industry, at least as protective as how we handle other confidential information. Measures include: - Encryption (AES-256+) - Access controls - Security assessments - Personnel training - Physical security - Data segregation - Timely breach notification

2.3. **Periodic Re-Consent.** To comply with laws and maintain accuracy, periodic re-consent (at least every 24 months) is required for continued storage/use of Biometric Data.

## 3. USER RIGHTS REGARDING BIOMETRIC DATA

3.1. **Right to Access.** You have the right to confirm processing and access your Biometric Data.

3.2. **Right to Deletion.** You may request deletion of your Biometric Data. SHMONG will permanently delete it from its systems within 45 days (subject to legal retention needs).

3.3. **Right to Withdraw Consent.** You may withdraw consent anytime. SHMONG will cease processing and delete your Biometric Data accordingly.

3.4. **Exercise Rights.** Contact Legal@shmong.com to exercise these rights. SHMONG will respond within legal timeframes (typically 45 days, extendable once).

3.5. **Data Removal Request Process.** Individuals may request complete Biometric Data removal: - **Uploader Responsibility**: As an uploader, you are solely responsible for all legal compliance related to biometric data consent, notification, and record-keeping. You must: - Establish a clear process for individuals in your Content to request removal - Collect sufficient information to verify identity - Maintain an immutable log of all removal requests for 3 years - Bear sole legal responsibility for any claims related to consent or improper collection - Indemnify SHMONG for any claims arising from your uploaded Content

- **SHMONG Technical Role**: Upon receiving a verified removal request (either directly or from an uploader), SHMONG will:
  - Execute the technical removal of biometric data from SHMONG systems
  - Complete removal within 30 calendar days from verification
  - Provide confirmation of technical deletion
  - Notify relevant service providers processing this data

  **Limited Technical Role Disclaimer**: SHMONG's execution of technical deletion does not in any way assume, transfer, or share the uploader's sole legal responsibility for consent collection, notification requirements, or compliance with biometric privacy laws. The uploader acknowledges and agrees they remain solely legally accountable for all consent-related matters regardless of who executes the technical deletion.

> **In Plain Language:** - If someone wants their face data removed, they can ask you (the uploader) or us directly - If asked, we'll delete their data within 30 days and confirm when it's done - Even though we'll delete the data when requested, uploaders remain fully responsible for having gotten proper permission in the first place - As an uploader, you need to have your own process for handling removal requests

## 4. DATA SHARING LIMITATIONS

4.1. **Commercial Data Usage and Rights.** SHMONG expressly reserves the right to the following, subject to state-specific limitations in Section 5: - Commercially use your biometric data as permitted by applicable law - Generate revenue from insights derived from biometric data - Share biometric data with service providers and partners as needed - Create and monetize products based on biometric data - Use anonymized biometric data for commercial purposes in all jurisdictions

“Anonymization” means the process of permanently removing all identifiers that could link biometric data to you personally. This includes removing names, account details, device identifiers, and applying technical measures to prevent re-identification. Anonymized data is transformed so it can no longer be associated with any specific individual.

By accepting this Agreement, you explicitly consent to these commercial activities to the extent permitted in your jurisdiction. The exact rights we exercise will depend on the laws of your state of residence.

4.2. **Limited Disclosure.** We will not disclose Biometric Data unless: - You consent - It completes a requested transaction - Required by law/valid legal process - To contractors/agents assisting us, who are contractually bound to confidentiality

## 5. STATE-SPECIFIC PROVISIONS

5.1. **Illinois Residents (BIPA).** For Illinois residents: - We will store, transmit, and protect biometric identifiers using reasonable care and in accordance with the Illinois Biometric Information Privacy Act (BIPA) - We will destroy biometric data within 3 years of last interaction or when the purpose is satisfied - We will not sell, lease, trade, or otherwise profit from your identifiable biometric information as prohibited by BIPA - Any commercial use of Illinois residents’ data will be strictly limited to properly anonymized data that cannot be re-identified - “Anonymization” for BIPA compliance means irreversibly removing or transforming all identifiers and applying

technical safeguards certified to prevent the data from being re-associated with your identity - By accepting this Agreement, you provide written release as required by BIPA solely for the collection, storage, and explicitly permitted uses of your biometric data - This written release does not authorize any use prohibited by BIPA - Illinois residents' biometric data will be handled with the highest level of protection required by BIPA

5.2. **Texas Residents (CUBI).** For Texas residents: - The purpose of collecting biometric identifiers is to provide face matching services for users to their images - We will destroy biometric identifiers within one year after this purpose expires, meaning one year after you stop using our face matching service or delete your account - We will store and protect biometric identifiers using reasonable care as required by Texas law - Texas law allows for commercial use of biometric data with proper consent - By accepting this Agreement, you provide consent for the sale, sharing, and commercial use of your biometric data as permitted by Texas law - You acknowledge you have been informed and give permission for these commercial uses - For additional protection, we may anonymize your data before certain commercial uses - "Anonymization" means permanently removing identifiers that could connect the data to you personally, making it impossible to re-identify you from the data

5.3. **California Residents (CCPA/CPRA).** For California residents: - Biometric Data is treated as sensitive personal information under California law - You have the right to limit use/disclosure of your biometric data - You have the right to opt-out of the sale or sharing of your biometric data - To exercise your "Do Not Sell/Share" right under California law, email Legal@shmong.com with the subject line "California Do Not Sell/Share" - We will process your request within 15 calendar days of receipt - You will not be discriminated against for exercising your California privacy rights - We provide this email mechanism as our required "Do Not Sell/Share" functionality for all California residents

5.4. **Additional States.** We commit to complying with applicable biometric/privacy laws in other states (WA, NY, CO, etc.) providing additional protections.

## 6. DATA SECURITY AND BREACH RESPONSE

6.1. **Technical Safeguards.** We implement specific safeguards for biometric data, including: - One-way encryption for biometric templates - Segregation from other user data - Multi-factor authentication for system access - Database-level encryption - Regular penetration testing - Zero-trust security architecture

6.2. **Breach Response Protocol.** In the event of a biometric data breach: - We will notify affected individuals within 72 hours of breach confirmation - We will notify regulatory authorities as required by law - We will provide description of the breach and types of data affected - We will outline steps taken to remediate the breach

## 7. INTERNATIONAL CONSIDERATIONS

7.1. **Cross-Border Data Transfers.** Your biometric data may be transferred to, stored, and processed in countries outside your country of residence, including the United States. For such transfers, we implement appropriate safeguards in accordance with applicable data protection laws, which may include: - Standard Contractual Clauses (SCCs) approved by the European Commission - Binding Corporate Rules (BCRs) where applicable - Data Transfer Impact Assessments (DTIAs) to assess and mitigate risks - Additional technical, organizational, and contractual measures as required - Country-specific transfer mechanisms as legally required

7.2. **European Union/EEA Users.** For EU/EEA residents: - We process biometric data based on your explicit consent as required by GDPR Article 9 - We implement appropriate technical and organizational security measures - We fully respect and facilitate all data subject rights under GDPR Articles 15-22 - We conduct and document data protection impact assessments - For cross-border transfers, we utilize European Commission approved SCCs with supplementary measures as recommended by the European Data Protection Board - We maintain records of all processing activities involving biometric data - We apply Privacy by Design principles to all biometric data processing

7.3. **UK Residents.** For UK residents, we comply with the UK GDPR and UK Data Protection Act 2018, including UK-specific data transfer mechanisms where relevant.

7.4. **Other International Jurisdictions.** We comply with applicable privacy and data protection laws in other countries regarding biometric data, including but not limited to: - Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) - Brazil's General Data Protection Law (LGPD) - Australia's Privacy Act - Japan's Act on the Protection of Personal Information (APPI) - South Korea's Personal Information Protection Act (PIPA)

## 8. BIOMETRIC ALGORITHM TRANSPARENCY

8.1. **Accuracy and Performance.** Our facial recognition technology: - Achieves 99.8% accuracy in controlled testing environments - Maintains 98.5% accuracy in real-world conditions with proper lighting - Has a false positive rate of less than 0.1% (1 in 1,000) - Has a false negative rate of approximately 1.5% - Performance metrics are regularly updated through continuous testing

8.2. **Demographic Performance.** Our commitment to fairness includes: - Testing across diverse demographic groups to identify and mitigate potential biases - Accuracy rates of 98.0-99.9% across different skin tones - Gender classification accuracy of 98.5% across gender expressions - Age group recognition accuracy of 97% across age ranges - Continuous algorithm improvement to address any identified disparities

8.3. **Testing Methodology.** Our facial recognition system is evaluated using: - Diverse test datasets representing various demographics - Real-world usage scenarios and lighting conditions - Independent third-party validation of performance metrics - Confusion matrix analysis for false positive/negative rates - Benchmarking against industry standards and datasets

8.4. **System Limitations.** We transparently acknowledge the following limitations: - Reduced accuracy in extremely low lighting conditions - Potential challenges with partial face occlusions - Performance variations with significant facial changes (injury,

surgery, aging) - Environmental factors such as glare or extreme angles may affect performance - Limitations processing multiple faces in crowded scenes with overlapping features

8.5. **Continuous Improvement.** Our facial recognition technology undergoes: - Regular retraining with diverse datasets - Quarterly bias audits and fairness evaluations - Performance benchmarking against industry standards - Feature engineering optimization based on user feedback

## 9. FACIAL RECOGNITION ETHICS STATEMENT

9.1. **Ethical Principles.** SHMONG is committed to the following ethical principles: - Human-centered approach prioritizing user dignity and rights - Fairness and non-discrimination across all demographic groups - Accountability through transparent practices and policies - User autonomy through informed consent and control - Privacy by design and default in all aspects of our service

9.2. **Prohibited Use Cases.** Our facial recognition technology shall not be used for: - Mass surveillance or monitoring of public spaces - Law enforcement or criminal investigation purposes without explicit legal process - Discrimination based on race, gender, religion, or other protected characteristics - Tracking individuals without their knowledge and consent - Evaluating eligibility for essential services, housing, or employment - Any purpose that violates fundamental human rights

9.3. **Algorithmic Fairness.** We maintain fairness through: - Regular auditing for potential biases across demographic groups - Diverse training datasets representing various populations - Transparency about performance variations across demographics - Regular testing by independent third parties - Ongoing adjustments to improve equity across all groups

9.4. **Human Oversight.** While we use automated systems: - Critical decisions involve human review - Regular human auditing of algorithmic performance - Users can request human review of

automated decisions - Human expertise is incorporated in system design and implementation - Staff training on ethical considerations and potential impacts

9.5. **Commitment to Research and Improvement.** We are dedicated to:

- Ongoing research into potential social impacts of facial recognition - Incorporating evolving ethical standards into our practices - Participating in multi-stakeholder dialogues on responsible AI - Publishing transparency reports on system performance - Continuous improvement based on emerging best practices

## DEFINITIONS

- **"Biometric identifier"**: A retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.
- **"Biometric information"**: Information based on an individual's biometric identifier used to identify an individual.
- **"BIPA"**: Illinois Biometric Information Privacy Act, which regulates the collection and use of biometric identifiers.
- **"CUBI"**: Texas Capture or Use of Biometric Identifier Act, which regulates biometric identifiers.
- **"CCPA/CPRA"**: California Consumer Privacy Act and California Privacy Rights Act, which regulate personal information, including biometric data.
- **"Encryption"**: The process of converting information into a code to prevent unauthorized access.
- **"One-way encryption"**: A form of encryption that cannot be reversed to recreate the original data.
- **"Zero-trust security"**: A security model that requires strict identity verification for every person and device.
- **"Data segregation"**: The separation of different types of data to enhance security and privacy.