Privacy Policy – Aura Chat

Last updated: August 1, 2025

General Information

This Privacy Policy describes how your personal data is collected, used, and protected when you use Aura Chat, our secure messaging service. We are committed to protecting your privacy and ensuring transparent communication about our data practices.

End-to-End Encryption

Messages and Content

- **Complete Encryption**: All messages are encrypted end-to-end using advanced cryptographic protocols before being transmitted and stored
- **Zero Knowledge**: We CANNOT and DO NOT read your messages - they remain completely unreadable to our systems and personnel
- **Access Control**: Only users possessing the correct chat code can decrypt and access message content
- **Username Protection**: All usernames are encrypted and stored in non-readable format on our servers
- **Automatic Security**: Encryption keys are automatically generated from unique chat codes using secure algorithms

What We CANNOT Access

- The actual content of your messages
- Your real identity or username in plain text
- Information about your conversation partners
- Any personal details shared within conversations
- Message metadata beyond technical requirements

Data Collection

Chat Codes

- We store chat codes (e.g., "Ab3$9Kl2") for technical system functionality
- Chat creation and expiration timestamps for maintenance purposes
- System metadata including creation dates and operational status
- No personal information is derivable from these technical identifiers

Authentication Data

- **Firebase Anonymous UID**: We collect and store your Firebase-generated anonymous user identifier
- This UID is a random technical identifier with no connection to your real identity
- It is essential for authentication services and system security
- Used exclusively for technical operations and user session management
- Cannot be traced back to personal information

Data Storage and Retention

Storage Period

- Chat data is retained only for the duration necessary to provide service functionality
- Anonymous Firebase UIDs are kept for technical and security purposes
- Data retention follows the principle of minimization - we keep only what's absolutely necessary
- No permanent archives of conversation content are maintained

Temporary Processing

- Message data exists temporarily during transmission and delivery
- No long-term backups of encrypted chat contents
- Data processing is strictly limited to core service functionality
- Automated deletion processes remove unnecessary data

Security Measures

Technical Protection

- Implementation of Firebase security with strict access rules and authentication protocols
- Multi-layer encryption using XOR algorithms combined with Base64 encoding
- Access restrictions ensuring only authenticated users can interact with their data
- Regular security audits and automated monitoring systems
- Protection against unauthorized access and data breaches

Security Considerations

- **User Responsibility**: Security effectiveness depends on maintaining chat code confidentiality
- **Access Control**: Never share chat codes with unauthorized individuals

- **Best Practices**: We recommend using strong, unique chat codes and avoiding sharing them through insecure channels

Data Usage and Purpose

Collection Purposes

Your data is collected and processed exclusively for:

- Providing reliable chat service functionality
- Ensuring technical system operation and performance
- Implementing necessary system maintenance and updates
- Maintaining security and preventing unauthorized access
- Complying with legal obligations where applicable

No Commercial Use

- We do NOT share, sell, or distribute your data to third parties
- We do NOT use your information for advertising or marketing purposes
- We do NOT analyze conversation content for commercial gain
- We do NOT create user profiles or behavioral tracking

Legal Basis (GDPR Compliance)

Under the General Data Protection Regulation (GDPR), our data processing is based on:

- **Consent**: Your voluntary use of the service constitutes informed consent to necessary data processing
- **Legitimate Interest**: Technical operation and security of the service represent legitimate business interests
- **Contractual Necessity**: Processing required to deliver the messaging service you've requested
- **Legal Compliance**: Meeting applicable legal and regulatory requirements

Your Privacy Rights

Available Rights

You have the following rights regarding your personal data:

- **Right of Access**: Request information about what data we store about you
- **Right to Rectification**: Request correction of inaccurate personal data
- **Right to Erasure**: Request deletion of your personal data ("right to be forgotten")

- **Right to Data Portability**: Request a copy of your data in a structured format (limited due to encryption)
- **Right to Object**: Object to processing based on legitimate interests
- **Right to Restrict Processing**: Request limitation of data processing in certain circumstances

Exercising Your Rights

To exercise any of these rights:

1. Contact us using the information provided in the Contact section
2. Provide sufficient information to verify your identity
3. Specify which right(s) you wish to exercise
4. We will respond within 30 days as required by law

Note: Due to our end-to-end encryption, some requests may be technically impossible to fulfill while maintaining security.

Technology and Infrastructure

Core Technologies

- **Firebase Realtime Database**: Secure cloud database for encrypted data storage
- **Firebase Authentication**: Anonymous authentication system for user management
- **Custom Encryption Protocol**: Advanced XOR encryption combined with Base64 encoding
- **Secure Transmission**: All data transmitted over encrypted HTTPS connections

Infrastructure Security

- Data centers with physical security measures
- Regular security updates and vulnerability assessments
- Compliance with industry-standard security practices
- Monitoring systems for unusual activity detection

International Data Transfers

- Data may be processed in various countries where our service providers operate
- We ensure adequate protection through appropriate safeguards
- All transfers comply with applicable data protection regulations
- Users are informed of the international nature of cloud services

Contact Information

For questions about this Privacy Policy, to exercise your rights, or for general privacy inquiries:

Email: aurastudio.italia@gmail.com
Data Controller: Aura Studio Italia
Response Time: We aim to respond to all privacy inquiries within 72 hours

Changes to This Privacy Policy

Update Process

- We reserve the right to modify this Privacy Policy to reflect changes in our practices or legal requirements
- Material changes will be prominently posted on our service
- The "Last updated" date at the top of this document indicates the most recent revision
- Continued use of the service after changes constitutes acceptance of the updated policy

Notification of Changes

- Significant changes may be communicated directly through the service
- Users are encouraged to review this policy periodically
- Previous versions may be available upon request

Agreement and Consent

By using Aura Chat, you:

- Acknowledge that you have read and understood this Privacy Policy
- Consent to the collection and processing of your data as described
- Understand the encrypted nature of the service and its security implications
- Agree to the terms and conditions outlined in this document

---

This Privacy Policy is effective as of the date indicated above and applies to all users of Aura Chat services.