

Another.IM — Privacy Policy

Effective date: 21.08.2026

Last updated: 21.08.2026

This Privacy Policy (the “Policy”) explains what data may be processed when you use the Another.IM application, website, XMPP infrastructure and related services (collectively, the “Service”), for what purposes such data is used, and what rights you have as a user.

The Service is provided by **Narayana OÜ**, registry code **12779661**, Väike-Paala 2, Tallinn, Harju County, Estonia, 11415 (“Another.IM”, “we”, “us” or “our”).

We aim to process personal data in accordance with applicable data protection laws, including the **General Data Protection Regulation (GDPR)**, where and to the extent it applies to the relevant processing activities.

1. Key Principles

Another.IM follows these principles when processing data:

- we aim to collect only the data necessary to operate the Service;
 - we do not require identity verification to create an account unless this becomes necessary in the future;
 - we do not sell users’ personal data;
 - we do not use the content of private messages for advertising;
 - when end-to-end encryption is used, we are not intended to have access to the content of properly encrypted messages;
 - we do not create backups of accounts specifically for the purpose of restoring them after deletion;
 - we implement technical and organizational measures designed to protect the data we process.
-

2. What Data We May Process

The specific data processed depends on how you use Another.IM.

2.1. Account Data

When you create an account, Another.IM may process data necessary to create and operate that account.

This may include:

- your XMPP JID or other account identifier;
- username;
- authentication data;
- data required for account recovery or security, where such functionality is provided;
- account settings;
- technical account parameters.

At this stage, Another.IM does not require KYC or mandatory identity verification.

We do not require passport details, residential address or other identity documents unless this is required for a specific feature or by applicable law.

3. Data Related to Your Use of the Service

When you use Another.IM, certain technical data may be collected automatically.

Depending on the architecture and configuration of the Service, this may include:

- IP address;
- connection date and time;
- network connection information;
- device type;
- operating system;
- application version;
- session identifiers;
- XMPP server information;
- technical logs;
- error and crash information;
- information necessary to maintain security and prevent abuse.

Not all of the data listed above is necessarily collected or retained in every case.

The exact categories of technical data collected and their retention periods will be determined after the Another.IM technical architecture has been finalized.

4. XMPP Data and Metadata

Another.IM uses the XMPP protocol for communication.

To deliver messages and operate the XMPP infrastructure, the server may need to process certain technical information.

Depending on the configuration, this may include:

- sender JID;
- recipient JID;
- presence/status information;
- information about connected devices;
- message delivery information;
- timestamps;
- data required for message routing;
- information related to communication with other XMPP servers.

Such information is necessary to provide the communication service and does not mean that Another.IM has access to the content of messages in plaintext.

5. Message Content

5.1. End-to-End Encrypted Messages

Another.IM supports end-to-end encryption technologies, including **OMEMO**, where supported by the relevant configuration.

When end-to-end encryption is functioning correctly, message content is encrypted on the sender's device and decrypted on the recipient's device.

In such cases, Another.IM **is not intended to have access to the plaintext content of the message**.

We do not use the content of end-to-end encrypted messages for advertising, user profiling or other purposes unrelated to providing the communication service.

5.2. Limitations

The use of end-to-end encryption does not mean that all data related to a communication is encrypted.

Certain metadata may be necessary for message delivery and operation of the XMPP infrastructure.

In addition, if you use a third-party XMPP server or client, the operation of that service is governed by the privacy policy of its operator.

6. Encryption Keys

The operation of OMEMO and other encryption mechanisms may require the processing of cryptographic keys and related data.

Depending on the architecture of the relevant version of Another.IM:

- private keys may be stored exclusively on users' devices;
- public keys and related data may be transmitted to an XMPP server;
- the server may store technical data required to deliver encrypted messages between devices.

The exact architecture for storing cryptographic keys will be specified in this Policy after it has been technically verified.

Another.IM should not make claims about being unable to access particular data until such claims have been confirmed by the actual implementation.

7. Files, Images and Other Attachments

Users may send files, images, video, audio and other attachments through Another.IM.

Depending on the transfer mechanism used:

- a file may be transferred directly between users;
- a file may be temporarily stored on a server;
- a file may be stored in separate storage infrastructure;
- the file may be protected using end-to-end encryption.

If a file is transferred using end-to-end encryption, its content should not be accessible to Another.IM in plaintext.

The specific file storage architecture and retention periods are subject to confirmation.

8. Data Voluntarily Provided by Users

Users may voluntarily provide additional information when interacting with Another.IM.

For example:

- email address;
- name;
- information provided to customer support;
- support requests;
- device information;
- information about a problem or error.

We use such information only for the purposes for which it was provided and in accordance with this Policy.

Providing additional information is generally not required to use the core functionality of the Service.

9. Data We Do Not Require

At this stage, Another.IM does not require users to provide:

- passport details;
- telephone number;
- residential address;
- payment information;
- identity verification;
- KYC information.

If additional information is required for specific features in the future, the relevant requirements will be reflected in this Policy or in additional terms.

10. How We Use Data

We may process data for the following purposes.

10.1. Providing the Service

To:

- create and manage accounts;
- connect users to XMPP servers;
- deliver messages;
- provide presence functionality;
- transfer files and media;
- support encryption functionality;
- synchronize data between devices;
- provide technical support.

10.2. Security

To:

- prevent abuse;
- detect suspicious activity;
- protect accounts;
- prevent spam;
- protect our infrastructure;
- investigate security incidents.

10.3. Improving the Service

We may use technical data to:

- analyze errors;
- diagnose crashes;
- improve stability;
- improve performance;
- develop new features.

If third-party tools are used for analytics, the relevant categories of data and providers will be identified in this Policy.

10.4. Compliance with Legal Obligations

We may process and retain data where necessary to:

- comply with applicable laws;
- comply with court orders;
- respond to lawful requests from government authorities;
- protect our legal rights;
- prevent fraud and other violations.

11. Legal Bases for Processing

Where the GDPR applies to our processing activities, we rely on one or more of the following legal bases.

Performance of a Contract

Where processing is necessary to provide the Service to you under the Terms of Service.

For example:

- creating an account;
- authentication;
- message delivery;
- technical maintenance of the Service.

Legitimate Interests

Where processing is necessary for our legitimate interests, such as:

- maintaining security;
- preventing abuse;
- protecting infrastructure;
- diagnosing technical issues;
- improving the reliability of the Service.

When relying on this legal basis, we consider your interests and fundamental rights.

Legal Obligation

Where processing is necessary to comply with applicable legal requirements.

Consent

Where applicable law requires consent, we will obtain it separately.

You may withdraw your consent at any time where processing is based on consent.

12. Sharing Data with Third Parties

We do not sell users' personal data.

We may share or provide access to certain data with the following categories of recipients:

- hosting providers;
- network infrastructure providers;
- technical support providers;
- abuse-prevention and security providers;

- analytics and diagnostic providers;
- other technical contractors necessary to operate the Service.

Such providers receive only the data necessary to perform the relevant functions.

We seek to use contractual and technical measures designed to protect users' data.

13. Third-Party XMPP Servers

Another.IM may be used with XMPP accounts hosted by third-party providers.

In such cases, certain information may be processed by the operator of the relevant XMPP server.

For example, a third-party server operator may have access to:

- JID;
- connection information;
- presence;
- technical metadata;
- encrypted data required for routing.

Another.IM's Privacy Policy **does not apply to the processing of data by third-party XMPP providers.**

You should review the privacy policy of the relevant provider.

14. International Data Transfers

Another.IM may use service providers whose infrastructure is located in different countries.

Where personal data is transferred outside the European Economic Area, we will use legally recognized transfer mechanisms, including, where applicable:

- European Commission adequacy decisions;
- Standard Contractual Clauses;
- other lawful mechanisms for international data transfers.

The specific countries and transfer mechanisms will depend on the infrastructure providers we use.

15. Data Retention

We retain data only for as long as necessary for the purposes for which it was collected, unless a longer retention period is required by law.

Retention periods depend on the type of data.

For example:

- account data — while the account exists;
- technical logs — for the period necessary for security, diagnostics and operation of the Service;
- customer support requests — for the period necessary to handle the request and protect our legitimate interests;
- data required to be retained by law — for the legally required period.

Specific retention periods for technical data will be determined after the Another.IM infrastructure has been finalized.

16. Account Deletion

Users may delete their account where the relevant functionality is available in the Service.

After deletion:

- the account will no longer be accessible to the user;
- account data will be deleted in accordance with the applicable deletion procedure;
- no account backup will be created or retained for subsequent restoration;
- data may be permanently lost.

Certain data may remain after account deletion if:

- required by law;
- necessary to comply with legal obligations;
- necessary to prevent fraud or abuse;
- necessary to establish, exercise or defend legal claims.

After the applicable retention period expires, such data will be deleted or anonymized.

17. Cookies and Similar Technologies

The Another.IM website may use cookies and similar technologies.

They may be used to:

- operate the website;
- remember user preferences;
- maintain security;
- analyze technical errors;
- obtain usage statistics.

The specific list of cookies and analytics tools will be provided in a Cookie Policy or in the relevant section of this Policy once the web infrastructure has been finalized.

18. Children

Another.IM is intended for users **13 years of age or older**.

We do not knowingly seek to collect personal data from children under 13.

If you believe that a child below the applicable age has provided us with personal data, you may contact us using the details below.

If we discover that we have collected such data without an appropriate legal basis, we will take reasonable steps to delete it.

19. Data Security

We implement reasonable technical and organizational measures designed to protect data against:

- unauthorized access;
- loss;
- alteration;
- disclosure;
- destruction.

These measures may include:

- encryption;
- access controls;
- authentication;
- infrastructure monitoring;

- restricted access for employees and contractors;
- technical measures to protect servers and networks.

However, no internet service can guarantee absolute security.

Users are also responsible for protecting their devices, passwords, encryption keys and other access credentials.

20. Data Breaches and Security Incidents

In the event of an incident involving personal data, we will act in accordance with applicable law.

Where the law requires us to notify users or a competent authority of such an incident, we will do so within the time limits required by law.

21. Your Rights

Where the GDPR or other applicable law grants you relevant rights, you may have the right to:

- access your personal data;
- request correction of inaccurate data;
- request deletion of your data;
- request restriction of processing;
- object to certain types of processing;
- receive your data in a portable format;
- withdraw previously provided consent;
- lodge a complaint with a competent supervisory authority.

Some of these rights may be limited by applicable law.

22. Exercising Your Rights

To exercise your rights, you may contact us at: support@another.im

We may request additional information necessary to verify your identity where this is required to protect your data against unauthorized access.

We aim to respond to requests within the time limits required by applicable law.

23. Complaints

If you believe that your personal data is being processed in violation of applicable law, you may first contact us to seek a resolution.

You also have the right to lodge a complaint with the relevant data protection authority.

For processing subject to the GDPR, this may be the supervisory authority in your country of residence or the relevant authority in Another.IM's jurisdiction.

24. Changes to This Privacy Policy

We may update this Policy from time to time.

Where material changes are made, we will notify users through the Service or publish an updated version on the Another.IM website.

The date of the latest update will be displayed at the top of this document.

Continued use of the Service after the changes become effective means that the user has reviewed the updated Policy, to the extent permitted by applicable law.

25. Contact Information

The Service is operated by:

Narayana OÜ

Väike-Paala 2

Tallinn, Harju County

Estonia, 11415

Registry code: **12779661**

For questions regarding the processing of personal data:

Email: support@another.im