Identity Server Privacy Policy.

1. Introduction

1.1. English, Not Legalese

Privacy is important, and we want you to understand the issues involved. We have decided to use plain English as much as possible, to make our terms as clear as possible.

When you read 'the Identity Server', 'the Identity Servers', or 'the Service' below, it refers to the Identity Servers made available at https://vector.im and https://matrix.org which provide account discovery services or Matrix users.

Where you read **'Roomys'** or **'we'** or **'us'** below, it refers to Roomys, a trading name of New Vector Ltd., its French subsidiary: Roomys Software SARL, its U.S. subsidiary: Roomys Software Inc, its German subsidiary: Roomys Software GmbH, and their agents.

The Matrix protocol is licensed by the Matrix Foundation which makes it available to third parties who set up their own Identity Server. This privacy notice does not apply to Matrix Identity Servers run by anyone else - Matrix is an open network like the Web and this agreement only applies to the Identity Servers (matrix.org and vector.im) provided by **Roomys**

Element is the Data Controller for the Service.

Email: support@roomys.io

Postal address:
Roomys **c/o New Vector Ltd 10 Queen Street Place**
London
United Kingdom
EC4R 1AG

Should you have other questions or concerns about this document, please send us an email at support@roomys.io.

1.2. This is a living document

With your help, we want to make our policy documents the best in the industry.

If you read something that rubs you the wrong way, or if you think of something that should be added, please get in touch! We're all ears! Email support@roomys.io and we'll chat.

We don't amend this document for any specific users or use case, but if your proposed changes apply to all of our users, we'll be happy to update it for everyone. Scroll to the bottom to see the history so far.

We will likely improve this document over time. By continuing to use the Service, you will implicitly accept the changes we make.

Your access and use of the Service is always subject to the most current version of this document.

2. What is a Matrix Identity Server?

Identity Servers support contact discovery on Matrix by letting people look up Third Party Identifiers to see if the owner has publicly linked them with their Matrix ID.

2.1. What is a Third Party Identifier?

A Third Party Identifier is an identifier that uniquely identifies a person, but *isn't* a Matrix ID. Most commonly this is an email address or a telephone number.

2.2. How does it support contact discovery?

Identity Servers offer the following services:

Verified Association of Matrix ID with Third Party Identifier

You can ask the Identity Server to establish that you own your email address or phone number and associate it with your Matrix ID. The Identity Server will verify that you own that identifier by sending a link or code to your email address or phone. The association is not considered valid until your ownership of the Third Party Identifier has been confirmed.

Account Lookup by Third Party Identifier

You can look up a Matrix ID by searching for its associated Third Party Identifiers. **You cannot look up Third Party Identifiers by searching for their associated Matrix ID.** For example: if Alice has used the Identity Server to link her email, alice@example.com with her Matrix ID, @example:matrix.org, other users can look up her Matrix ID by querying the Identity Server with her email address, but *they cannot discover her email address by querying the service with her Matrix ID*.

The Identity Server supports both individual and bulk Third Party Identifier lookup:

Individual Third Party Identifier Lookup

Individual Third Party Identifier Lookup is usually used when inviting a user to a Matrix room by their Third Party Identifier.

Bulk Third Party Identifier Lookup

Bulk Third Party Identifier Lookup is usually used to check whether any of your existing contacts already have a Matrix ID.

Registration with Email or Phone Number

Some homeservers rely upon the Identity Server for part of new user registration, using the Identity Server to perform the verification of ownership of the email address or phone number.

We will be removing support for user registration from the Roomys **Identity Servers.** In the near future homeservers we manage will be able to complete registration by email address without delegating ownership verification to an Identity Server. This document will be updated when this behaviour has changed.

Password Reset

Some homeservers rely upon the Identity Server for password reset by email, using the Identity Server to send a unique link to the user to complete password reset securely.

We do not provide support for password reset from the Roomys **Identity Servers.** Homeservers can already complete password reset by email without delegating to an Identity Server. Homeserver administrators should not rely on **Roomys** Identity Servers for password reset.

Binding on Registration

When your client is configured to use either the vector.im or the matrix.org Identity Server and you register on a homeserver with your email address and/or phone number:

- if that homeserver is run by **Roomys** (e.g. the homeserver running at matrix.org, or a Roomys Matrix Services homeserver), the corresponding homeserver privacy policy will advise you that the act of registration will *also* publicly link your email address and/or phone number with your Matrix ID via the Identity Server

- if that homeserver is **not** run by **Roomys** then registration will **not** publicly link your email address or phone number with your Matrix ID. In this case the vector.im or matrix.org Identity Server will only store your data long enough to establish your ownership of the Third Party Identifier.

This behaviour is also being phased out. In the near future, choosing to publicly link your Third Party Identifiers with your Matrix ID via an Identity Server will be a wholly separate step, fully divorced from registration. This document will be updated when this behaviour has changed.

2.3. Closed federation between Vector.Im and Matrix.org Identity Servers

Data is shared between the vector.im and matrix.org Identity Servers in a closed federation.
This means that when you ask the Identity Server at vector.im to link your Matrix ID with your email address or phone number, this data is replicated on the matrix.org Identity Server. Likewise if you ask the Identity Server at matrix.org to link your Matrix ID with your email address or phone number, this data is replicated onto the vector.im Identity Server.

3. Access to your data / Privacy Policy

3.1. What is the legal basis for processing my data and how does this affect my rights under GDPR (General Data Protection Regulation)?

3.1.1. Legal basis for processing

Roomys

Your data is processed under Legitimate Interest. This means that we process your data only as necessary to deliver the Service, and in a manner that you understand and expect.

The *Legitimate Interest* of the Service is the discoverability of contacts across the wider Matrix ecosystem. The processing of user data we undertake is necessary to provide the Service. **This facility is an optional component of the services provided by Roomys,** designed to make contact discovery easier. Matrix works very well without an Identity Server.

3.1.2. Right to erasure

You can remove your data from the Service at any time by using a Matrix client (such as Roomys) to remove your Third Party Identifiers from the connected Identity Server. The data will be rendered inaccessible across matrix.org and vector.im Identity Servers straight away, and will be deleted from the matrix.org and vector.im databases within 30 days.

If your homeserver is spec-compliant (i.e. if it faithfully implements the Matrix protocol specification detailed at https://matrix.org/spec), your Third Party Identifiers will be deleted if your account is deactivated.

3.1.3. Data portability

Under GDPR you have a right to request a copy of your data in a commonly-accepted format. If you would like a copy of your data, please send a request to support@roomys.io.

3.1.4. Your rights as data subjects

You have rights in relation to the personal data we hold about you. Some of these only apply in certain circumstances. Some of these rights are explored in more detail elsewhere in this document. For completeness, your rights under GDPR are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

For more details about these rights, please see the guidance provided by the ICO. If you have any questions or are unsure how to exercise your rights, please contact us at support@roomys.io.

3.2. What information do you collect about me and why?

The information we collect is purely for the purpose of letting people discover Matrix IDs that have been publicly linked with a Third Party Identifier (such as email or telephone number). We do not profile users or their data on the Service.

3.2.1. Information you provide to us:

We collect information about you when you input it into the Service or otherwise provide it directly to us.

- Matrix ID
- Third Party Identifiers (such as email or telephone number)

3.2.2. Information we collect automatically as you use the service:

Third Party Identifiers you look up

Third Party Identifiers that are looked up are logged in our application logs. These logs are kept for not longer than 7 days. Haproxy logs may be kept for up to 60 days.

Connection Information

Currently, we log the IP address of the party who accesses the Service. Since this is usually the homeserver requesting data on behalf of its user(s), it is usually the IP address of the homeserver that is logged. This data is used in order to mitigate abuse, debug operational issues, and monitor traffic patterns. Our logs are kept for no longer than 180 days.

3.3. What information is shared with third parties and why?

3.3.1. Sharing data with connected service

The purpose of the Service is to share your associated Matrix ID with whomever looks up your linked Third Party Identifiers. As a reminder, use of this service is optional - if you do not want your Matrix ID to be discoverable from your Third Party Identifiers, please do not use the service.

3.4. Sharing data in compliance with enforcement request and applicable laws; enforcement of our rights

In exceptional circumstances, we may share information about you with a third party if we believe that sharing is reasonably necessary to

- comply with any applicable law, regulation, legal process or governmental request,
- protect the security or integrity of our products and services (e.g. for a security audit),
- protect Roomys, The Matrix.org Foundation, and our users from harm or illegal activities, or

- responding to an emergency which we believe in good faith requires us to disclose information to assist in preventing the serious bodily harm of any person.

3.5. Our commitment to children's privacy

We never knowingly collect or maintain information in the Service from those we know are under 16, and no part of the Service is structured to attract anyone under 16. If you are under 16, please do not use the Service.

3.6. How can I access or correct my information?

You can view and modify your published Third Party Identifiers by using any compatible Matrix client (such as Roomys) and managing your User Settings.

3.7. Who can see my Matrix ID / Third PArty Identifier associations?

Anyone who knows your Third Party Identifier can query the Service to see if you have publicly linked it with a Matrix ID. Queries *only work in this direction* It is not possible for parties who only know your Matrix ID to query the service and discover your Third Party Identifiers.

The association between your Matrix ID and your Third Party Identifiers is stored in **Roomys** databases. This means that, unlike regular users, **Roomys** employees and contractors can look up your Third Party Identifiers from your Matrix ID (subject to the New Vector data access guidelines below).

3.8. What are the guidelines Roomys follows when accessing my data?

- We restrict who at **Roomys** (employees and contractors) can access user data to roles which require access in order to maintain the health of the Service.
- We never share what we see with other users or the general public.

3.9. Who else has access to my data?

We host the vector.im and matrix.org Identity Servers on UpCloud datacentres in London. Here's UpCloud's privacy policy. UpCloud controls physical access to their locations.

We use Cloudflare to mitigate the risk of DDoS attacks. Here's CloudFlare's privacy policy.

Physical access to our offices and locations use typical physical access restrictions.

We use secure private keys when accessing servers via SSH, and protect our console passwords locally with a password management tool.

We log application data (caller IP and user agent). We keep logs for no longer than 60 days.

3.10. What happens if Roomys is sold?

In the event that we sell or buy any business or assets, we may disclose your personal data to the prospective seller or buyer of such business or assets.

If we or substantially all of our assets are acquired by a third party, personal data held by us about our users will be one of the transferred assets.

3.11. How is my data protected from another user's data?

All of our users' data for the Service currently resides in the same database cluster. We use software best practices to guarantee that only people who know your linked Third Party Identifiers can use them to look up your Matrix id. In other words, we segment our user data via software. We do our best and are very confident we're doing a good job at it, but, like every other service that hosts their user data on the same database, we cannot guarantee that it is immune to a sophisticated attack.

3.12. What should I do if I find a security vulnerability in the service?

If you have discovered a security concern, please follow the Matrix.org Security Disclosure Policy.

4. Making a complaint

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention at support@roomys.io if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

If you want to make a complaint about the way we have processed your personal information to the supervisory authority, you can contact the ICO (the statutory body which oversees data protection law) at https://www.ico.org.uk/concerns.

5. Document History

- 2022, December 20: current version derived from previous Data Processing Agreement.
- 2023, June 23: Format updates.